CH 8-1. Purpose

The Defense Acquisition Guidebook (DAG), Chapter 8, provides guidance on the process and procedures for managing risks through planning and executing an effective and affordable test and evaluation (T&E) program that enables the Department of Defense (DoD) to acquire systems that work. With a robust and rigorous T&E program, engineers and decision-makers have the knowledge and support they need to manage risks, measure progress, and characterize operational effectiveness, operational suitability and survivability (including cybersecurity), or lethality.

The fundamental purpose of test and evaluation (T&E) is to enable the DoD to acquire systems that work. To that end, T&E provides engineers and decision-makers with knowledge to assist in managing risks, to measure technical progress, and to characterize operational effectiveness, operational suitability and survivability (including cybersecurity), or lethality. This is done by planning and executing a robust and rigorous T&E program. The objective of a T&E program is to characterize system capabilities across the intended operational conditions, verify that testable requirements are met or not met, and inform decision-makers, in accordance with DoDI 5000.02 (Encl. 4, para 2(a) – page 64). To that end, T&E enables the DoD to: acquire systems that work, provide engineers and decision-makers with knowledge to assist in managing risks, measure technical progress, and characterize operational effectiveness, operational suitability, and survivability (including cybersecurity), or lethality of the system in the intended operational environment. This is done by planning and executing a robust and rigorous T&E program.

CH 8–2. Background

The determination of how much and what kind of testing is sufficient for a program is a core challenge to the development of any T&E strategy. A new technical effort or a significant improvement in capability over a current system may require a significant amount of effort in developing the system. Therefore, programs need a comprehensive T&E strategy to inform acquisition decisions. In assessing the level of evaluations necessary, consider the maturity of the technologies used, the complexity of integration, and the operational environment of the system.

CH 8–2.1 T&E Strategy

The strategy for T&E begins with a review and understanding of the threat and the requirements. Program managers devise a T&E strategy generating the knowledge necessary for the acquisition, programmatic, operational, technical, and life-cycle support decisions of a program. Forming an effective T&E strategy requires careful analysis to determine the appropriate scope and depth of evaluations to be completed. This approach to T&E strategy development is to plan for the evaluation before testing, execute the test program, and conduct the evaluation as test data become available. This creates an environment where the evaluation guides the formulation of test objectives, configurations, conditions, data requirements, and analysis to develop information in support of the decision-making process.

Scientific Test & Analysis Techniques (STAT) should be used in designing an effective and efficient T&E program, in accordance with DoDI 5000.02 (Encl. 5, para 5(e) – page 101), in order to balance risk and the level of knowledge required for evaluations.

A non-developmental item (i.e., Commercial-Off-The-Shelf (COTS) or Government-Off-The-Shelf (GOTS)) still requires evaluation to assess capability. This may not involve much testing, but needs to ensure the item meets advertised capability, maturity, integration, and interoperability requirements. Therefore, developmental testing may be limited in scope, with operational testing focusing on the operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality of the system in the intended operational environment.

Evaluation assessments also address key risks or issues associated with sustaining the system capability in operational use, as well as the overall logistics effort, maintenance (both corrective and preventative), servicing, calibration, and support aspects.

CH 8–2.2 DoD T&E Organizations

The Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)) develops policy and guidance for developmental test and evaluation (DT&E) within the Department of Defense (DoD). The DASD(DT&E) also serves as the Director, Test Resource Management Center (TRMC) for oversight of DoD T&E resources and infrastructure. The DASD(DT&E) closely coordinates with the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)), and routinely coordinates with other Office of the Secretary of Defense (OSD) organizations.

The Director, Operational Test and Evaluation (DOT&E) provides oversight of operational test and evaluation (OT&E), and live fire test and evaluation (LFT&E), for programs on the DOT&E Oversight List, in accordance with DoDI 5000.02 (Encl. 5, para 3(a) – page 70). The DOT&E is responsible for generating OT&E and LFT&E policy for all programs within the DoD.

In accordance with 10 USC 139 (para e(2)) and DoDI 5134.17, the Secretary of Defense (SecDef) ensures both DASD(DT&E) and DOT&E have access to all records and data of the DoD (including the records and data of each Military Department and including classified and proprietary information, as appropriate) that they consider necessary in order to carry out their respective duties.

The DASD(DT&E) and DOT&E share or coordinate on the following responsibilities:

- Prescribe policies and procedures for T&E within the DoD.
- Provide advice, assessments, and recommendations to the SecDef, DepSecDef, and USD(AT&L), as well as support Overarching Integrated Product Teams (OIPTs) and Defense Acquisition Boards (DABs)/Information Technology Acquisition Boards for programs.
- Assess the adequacy of T&E strategies and plans for programs on the major defense acquisition program (MDAP), major automated information system (MAIS), AT&L Special Interest list, and DOT&E Oversight Lists by approving or disapproving Test and Evaluation Master Plans (TEMPs).
- Monitor and review DT&E, OT&E, and LFT&E events to assess adequacy of test planning, identify test execution issues, assess progress of T&E efforts, and obtain data for separate evaluations.
- Participate in the Developmental Test Readiness Review (TRR) and Operational Test Readiness Review (OTRR) process by providing assessments and recommendations concerning a system's readiness for operational testing.
- Provide assessments of system performance, T&E, and interoperability/information security for the Defense Acquisition Executive Summary (DAES) process.
- Assist program managers (PMs) in developing, assessing, and updating their T&E strategy, schedule and resources, and evaluating system performance.

CH 8–2.2.1 DASD(DT&E)

The Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)) serves as the principal advisor to the SecDef and the USD(AT&L) for DT&E in the DoD; and, as such, has responsibilities and duties as prescribed in DoDI 5134.17 (1(b) – page 3), Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)). Refer to DASD(DT&E) for additional information. In this capacity, the DASD(DT&E) shall:

- Develop policies and guidance for:
  - The planning, execution, and reporting of DT&E in the DoD, including integration and DT&E of software.
  - The integration of developmental and operational tests in coordination with the Director, Operational Test & Evaluation.
  - The planning, execution, and reporting of DT&E executed jointly by more than one Military Department or Defense Agency.
  - The use of DT&E planning principles and best practices.

    - Development of TEMPs in conjunction with the DOT&E.
    - Inclusion of provisions in Requests for Proposals (RFPs) that relate to DT&E.
    - The use of DT&E approaches to effectively support reliability growth programs.
    - The reporting of DT&E results to the DASD(DT&E) and USD(AT&L).
- Provide advice and make recommendations to the Secretary of Defense and the USD(AT&L) regarding DT&E and the execution of these activities within and across defense acquisition programs.
- Provide guidance to defense acquisition programs for developing and documenting the program's evaluation strategy and management approach in the TEMP throughout the program's life cycle.
- Act as an advisory member of the Defense Acquisition Board (DAB) and other key acquisition bodies; provide independent assessments of program DT&E, execution, and risk.
- Provide a recommendation to approve or disapprove the MDAP DT&E plans as well as advise the relevant technical authorities for these programs on the incorporation of best practices for developmental test from across the Department.
- Beginning with the Materiel Development Decision, monitor the development test and evaluation program activities of Major Defense Acquisition Programs (MDAPs) and review the DT&E plans for those programs in the TEMP.
- Serve as the T&E Functional Leader for the T&E acquisition career field within the DoD, providing advocacy, oversight, and guidance to elements of the acquisition workforce responsible for test and evaluation.
- Inform the Joint Capabilities Integration and Development System (JCIDS) process to ensure key technical requirements are measurable, testable, and achievable.
- Inform the DAES process.
- Submit, not later than March 31 of each year, to the congressional defense committees, an annual report as outlined DoDI 5134.17 (Encl. 1, para 1(l)).
- Consult with the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) on technological maturity and integration risk of critical technologies of MDAPs.
- Periodically review the organizations and capabilities of the Military Departments with respect to DT&E and identify needed changes or improvements to such organizations and capabilities.

CH 8–2.2.2 Office of the D,OT&E

The Office of the Director, Operational Test and Evaluation (D,OT&E), a principal staff assistant and advisor to the Secretary of Defense, has specific responsibilities assigned by 10 USC 139 and 2399 for OT&E and 10 USC 2366 for LFT&E. Additional responsibilities are identified in DoD Directive (DoDD) 5141.02, Director of Operational Test and Evaluation.

For purposes here, DOT&E:

- Prescribes policies and procedures for the conduct of OT&E and LFT&E for DoD.
- Monitors and reviews OT&E and LFT&E activities in the DoD.
- Exercises oversight responsibility for ACAT I or other programs in which the SecDef has special interest or for which DOT&E determines oversight is required, in accordance with DoDI 5000.02 (Encl. 5, para 3(a) – page 70).
- Publishes the DOT&E Oversight List, which identifies all programs under oversight for OT&E and/or LFT&E.
- Assesses the adequacy of OT&E and LFT&E performed by the Services and Operational Test Agencies (OTAs) for programs under DOT&E oversight.
- Approves the TEMP for oversight programs.
- Approves, in writing, the adequacy of operational test plans for those programs under DOT&E oversight prior to the commencement of operational testing.

- Approves, in writing, the use of data collected outside an approved operational test plan for use in operational evaluation.
- Approves LFT&E strategies and waivers prior to commencement of LFT&E activities.
- Approves the quantity of test articles required for operational testing of MDAPs; to include what is production representative for purposes of adequate and realistic OT&E, for programs on DOT&E oversight.
- Independently assesses the adequacy of testing and the operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality of programs under oversight.
- Provides independent reports to the SecDef, Congress, and USD(AT&L), among others, to support acquisition and operational decisions.
- Submits a report to the SecDef and Congress before systems on OSD DOT&E Oversight may proceed Beyond Low Rate Initial Production (BLRIP).
- Advises the DoD Executive Agent for Space and the acquiring Military Department on T&E of DoD Space MDAPs and other space programs designated for T&E oversight, in support of DoDD 3100.10, Space Policy (Encl. 2, para 3(a) –page 8).
- Provides support to the Director, Joint Improvised-Threat Defeat Organization (JIDO), consistent with DoDD 2000.19E, Joint Improvised Explosive Device Defeat Organization (JIEDDO) (Para 6.12 – page 8).
- Oversees and assesses operational capability demonstrations conducted by the Missile Defense Agency (MDA), consistent with DoDD 5134.09, Missile Defense Agency (MDA) (Para 6(c)(18)(b) – page 5).
- Establishes policy on the verification, validation, and accreditation (VV&A) of models and simulations used in support of OT&E and LFT&E.
- Oversees the International T&E (IT&E) program for the SecDef.
- Oversees and prescribes policy, as appropriate, to ensure adequate usage and verification of protection of human subjects and adherence to ethical standards in OT&E and LFT&E, in support of DoDD 3216.02, Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research (Part II – page 36).
- Assists and advises the Chairman of the Joint Chiefs of Staff (CJCS) in efforts to ensure the JCIDS documents, in terms verifiable through testing or analysis in support of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01I, (Para 4(f)(7) – page 4), Joint Capabilities Integration and Development System, provides the expected joint operational mission environment, mission level measures of effectiveness (MOEs), and key performance parameters (KPPs).
- Manages:
    - Efforts to improve interoperability and cybersecurity in the department through the operational evaluation of the systems under oversight and major exercises conducted by the combatant commands and the Military Departments.
    - Joint Test and Evaluation (JT&E) program (DoD Common Access Card (CAC) required).
    - Joint Live Fire program.
    - Center for Countermeasures.
    - Activities of the Joint Aircraft Survivability program.
    - Activities of the Joint Technical Coordinating Group for Munitions Effectiveness and producing the Joint Munitions Effectiveness Manual.
    - Activities of the T&E Threat Resource Activity.

The DOT&E prescribes policies and procedures for the conduct of OT&E and LFT&E in the DoD, in accordance with 10 USC 139 and 2366, respectively. For programs under DOT&E oversight, DOT&E

serves as the final approval authority for OT&E and LFT&E planning, including approval of the TEMP. DOT&E staff representatives provide advice to, and actively participate in, acquisition program T&E Working-Level Integrated Product Teams (WIPTs). DOT&E is a member/advisor of both the Joint Requirements Oversight Council (JROC) and the OIPT, providing advice and recommendations at DAB reviews; and has direct access to both USD(AT&L) and the SecDef, on all matters relating to OT&E.

PMs initiate early engagement with DOT&E through the Service and Defense Agency T&E Executives and independent Operational Test Agencies (OTAs). PMs also charter a T&E WIPT to aid in development of strategies for T&E and the TEMP. Since OT&E acts as a validation process for Systems Engineering, early engagement of the OTA and DOT&E is essential. Also, an early comprehensive assessment of the Analysis of Alternatives and any emerging requirements documents helps clarify and ensure the rationale, measurability, and testability of requirements, and clarify the associated implications to cost and schedule. These actions require close and continuous coordination with users, sponsors, developers, and all potential test organizations to ensure correct understanding and articulation of end-game expectations during program planning and documentation.

DOT&E approves all OT&E plans for all programs on the DOT&E Oversight List, including, but not limited to, early operational assessments (EOAs), operational assessments (OAs), Limited User Tests (LUTs), IOT&E, and Follow-on Operational Test & Evaluation (FOT&E). In accordance with 10 USC 139, OTAs provide DOT&E plans to assess adequacy of data collection and analysis planning to support DOT&E's independent assessment of a system's operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality. Additionally, OTAs schedule a test concept briefing at least 180 days prior to the anticipated start of an operational test. OTAs provide OT&E plans for DOT&E approval at least 60 days prior to the start of test events.

In accordance with 10 USC 139, the D,OT&E approves the number of low-rate initial production (LRIP) systems required for adequate operational testing of programs on the DOT&E Oversight List. For programs not on DOT&E oversight for operational testing, the Service OTA determines the number of LRIP systems required for OT&E. DOT&E and the OTAs routinely engage the PM in those decisions. For programs not on the DOT&E Oversight List, the Service or Defense Agency OTA works with the PMs for OT&E, including planning, applicable oversight, and execution and reporting; in accordance with DoDI 5000.02 (Encl. 5, para 3(a) – page 70).

In accordance with 10 USC 2399 (Para a), an MDAP must complete IOT&E before proceeding beyond LRIP.

In accordance with DoDD 5141.02 (Para 6(c) – page 5), in addition to OT&E oversight, the SecDef charges DOT&E with approving waivers to Full-Up, System-Level (FUSL) LFT&E and approval of required alternative LFT&E plans prior to Milestone B. For more detailed information on the waiver process, see DAG CH 8.3.2.5.5., Full-up, System-Level Testing Waiver Process.

Refer to DOT&E for additional information.

CH 8–2.2.3 Test Resource Management Center

In accordance with DoDI 5134.17 (Encl. 1, para 1(a)), the DASD(DT&E) serves concurrently as Director, Test Resource Management Center (TRMC), a field activity reporting directly to the USD(AT&L). 10 USC 196 (Para c) and DoDD 5105.71, Department of Defense Test Resource Management Center (TRMC), define the specific responsibilities of the TRMC, including the planning for, and assessment of, the adequacy of the Major Range and Test Facility Base (MRTFB). TRMC maintains awareness of other T&E facilities and resources, within and outside the DoD, and their impacts on DoD test capability in support of development, acquisition, fielding, and sustainment of defense systems. Within TRMC, the T&E Range Oversight (TERO) staff provides expertise on the MRTFB and assists DASD(DT&E) staff specialists in the review of TEMPs for adequacy of test infrastructure supporting a program's T&E. Bi-annually, TRMC produces the DoD T&E Resources Strategic Plan to inform DoD and Congress about the projected future of the T&E infrastructure's capability, to fulfill the T&E needs of the department. DoDI 3150.09, The

Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy, (Encl. 2, para 8(c) – page 14), states that TRMC assesses T&E infrastructure to ensure CBRN survivability test capabilities and resources are adequate or gaps are identified for investments.

TRMC oversees the MRTFB in accordance with responsibilities found in DoDD 3200.11, Major Range and Test Facility Base (MRTFB).

CH 8–2.2.3.1 Major Range & Test Facility Base

The Major Range and Test Facility Base (MRTFB) is the designated core set of DoD T&E infrastructure (open-air ranges, test facilities, instrumentation data processing, and other test resources) and associated workforce to provide T&E capabilities in support of the DoD acquisition system. The DoD, through the TRMC, oversees sustainment of all MRTFB T&E organizations or activities with a skilled workforce, and T&E technical capabilities and processes. MRTFB capabilities are available to all components under a common charge policy defined in DoD 7000.14-R, FMR Volume 11A, CH 12. Funding of MRTFB activities is designed to:

- Assure the most cost effective development and testing of materiel.
- Provide for inter-Service compatibility, efficiency, and equity without influencing technical testing decisions or inhibiting legitimate and valid testing.

The MRTFB is described in DoDD 3200.11, Major Range and Test Facility Base (MRTFB), and operates in accordance with DoDI 3200.18, Management and Operation of the Major Range and Test Facility Base (MRTFB). The Director, TRMC publishes for the SecDef the composition of the MRTFB activities, which can be found in DoDD 3200.11 (Para 5.1.2. – page 3). The TRMC TERO staff can assist in assessing MRTFB capabilities for programs through the DASD(DT&E) staff specialist participating in the T&E WIPT, or program managers can query TRMC directly through the TERO mailbox at: osd.pentagon.ousd-atl.mbx.trmc-tero@mail.mil.

CH 8–2.2.3.2 Non-Major Range & Test Facility Base Capabilities

DoDI 5000.02 (Encl. 4, para 5(b) – page 68), instructs programs to use government T&E facilities, unless an exception can be justified as cost-effective to the government. When programs consider locations to best accomplish T&E within budget and schedule, they start with MRTFB activities. MDAPs and MAIS rely on T&E facilities and other infrastructure owned and managed by the Services for a majority of their T&E infrastructure needs, and for the Lead DT&E Organization to determine and arrange for participating test organizations (MRTFB and non-MRTFB), as needed, to complement their capabilities to fully execute the T&E program. Reimbursement rates for use of all DoD or government T&E capabilities are subject to DoD 7000.14-R, FMR Vol.11A, CH 12. Use of or investment in commercial test capabilities requires a Cost Benefit Analysis (CBA) before incorporating or scheduling test plans. The TEMP articulates a concise summary of the CBA for the use of any commercial test facilities.

DoD does not provide a single source catalog of DoD T&E capabilities. For MDAPs, the Lead DT&E Organization should have knowledge of all government test resources for testing similar technologies and commodities, and should be able to advise the Chief Developmental Tester and the T&E WIPT of their recommendations. The Lead DT&E Organization can, if needed, query TRMC or contact TRMC directly for assistance in assessing potential test facilities and ranges via e-mail at: osd.pentagon.ousd-atl.mbx.trmc-tero@mail.mil with the subject line: “Test Capabilities Directory Assistance Request.” In the e-mail, provide program or organization name, short description of T&E capability needed, and an e-mail and phone number for the point of contact requesting information. A TERO staff support agent will assist in your T&E capabilities query.

Table 1 provides a list of T&E capability links, by DoD Component.

Table 1: DoD T&E Capability Links

ARMY	Army Test and Evaluation Command (ATEC) This site links to Army MRTFB sites as well as some non-MRTFB sites.
NAVY	Naval Air Systems Command (NAVAIR) Request contact information for NAVAIR 5.0 Test and Evaluation.
	Naval Sea Systems Command (NAVSEA) Reference the “Pocket Guide” for Warranted Technical Authorities listing or request contact information for the SEA 05B R&SE T&E office.
	Marine Corps Systems Command (MARCORSYSCOM) Request the Command Officer of the Day provide contact information for T&E in Deputy Commander Systems Engineering, Interoperability, Architectures & Technology (DC SIAT) office.
	SPAWAR Request contact information from Navy N84.
AIR FORCE	AFOTEC
OTHER	Range Commanders Council (RCC) Links to various DoD range facilities. The Secretariat may be able to provide contact information for various RCC members or Standing Groups.

CH 8–2.2.3.3 Joint Mission Environment Test Capability

The Joint Mission Environment Test Capability (JMETC) program’s mission is to provide a DoD-wide capability for distributed T&E of warfighter capabilities in a Joint context for interoperability, cybersecurity, KPP compliance testing, developmental testing (DT) and operational testing (OT), as well as Joint Mission Capability Portfolio testing, in accordance with DoDI 5000.02 (Encl. 4, para 3(f) – page 66). The program provides a test infrastructure necessary to conduct distributed test events integrating live, virtual, and constructive (LVC) test resources configured to support the users' needs. Distributed testing provides for near real-time “Test-Fix-Test” and integrated DT and OT methods that can provide early discovery of system problems. JMETC provides a dedicated help desk, common integration software for linking sites, accredited test tools, and distributed testing subject matter experts (SMEs) to support users with requirements development, test planning, cybersecurity, network troubleshooting, and use of test tools.

In the fall of 2012, TRMC assumed responsibility and funding for the National Cyber Range (NCR). The NCR provides a high-fidelity, realistic cyber environment to conduct sophisticated cyber training and support for cyber testing during all phases of the system life cycle as well as testing of complex system-of-systems. The NCR supports the ability to design, deploy, and sanitize large-scale, high-fidelity test and training environments in which malicious threats can be released on operationally representative systems and networks to assess their impact. The NCR provides the capability to emulate military and adversary networks at a relevant level of sophistication needed to execute realistic cyber tests, as well as cyber

mission rehearsals. An integrated tool suite provides automation and the ability to support multiple concurrent events, executed in isolated test beds at different levels of classification. NCR SMEs are available, at the discretion of the user, to support the planning, execution, and analysis of test and training events. The NCR has the capability to collaborate/integrate with other cyber ranges using secure networks when test events require special capabilities, additional scale, or connectivity to remote sites or assets.

For contact information and a map of JMETC distributed capabilities, locate the "Interoperability & Cyber Test" link on the DASD(DT&E)/Director, TRMC website, or directly from the JMETC website (Requires JMETC account).

CH 8–2.3 Component T&E Organizations

This section provides information on the varying DoD and Service T&E organizations, as highlighted in DoDI 5000.02 (Encl. 4 – page 64) and DoDI 5000.02 & Encl. 5 – page 69), and provides information on their functions and responsibilities.

CH 8–2.3.1 Army T&E Executive

The Army T&E Executive is the Director, T&E Office under the authority, direction, and control of the Deputy Under Secretary of the Army. Army Regulation (AR) 73-1 (CH 2 (2-1) – page 2) [NOTE: due to authentication controls, you must start from Army ePubs page and search in Publications/Administrative/Army Regulations for AR 73-1.] lists key Army T&E Executive duties and responsibilities include:

- Serving as the senior advisor to the Secretary of the Army and the Chief of Staff, Army, on all Army T&E matters.
- Advising the Army Systems Acquisition Review Council (ASARC), the Army Requirements Oversight Council (AROC), and OIPTs on T&E matters.
- Approving test-related documentation for the Secretary of the Army and forwarding, as appropriate, to OSD.
- Coordinating T&E matters with the Joint Staff and OSD, including serving as the principal Army interface on matters of T&E with the USD(AT&L) and DOT&E.
- Overseeing all Army T&E missions and functions, to include formulating overarching Army T&E strategy, policy, and program direction; providing policy oversight, and management of resources.
- Providing Headquarters, Department of the Army oversight on the funding of the Army Threat Simulator program, Army Targets program, and Army Instrumentation program.
- Overseeing Army responsibilities in Joint T&E, Foreign Comparative Testing (FCT), and multi-Service and multi-national T&E acquisition programs.
- Serving as the Army T&E functional chief for the T&E acquisition workforce career field.

CH 8–2.3.2 Air Force T&E Executive

The Air Force T&E Executive serves as the Director, Air Force Test and Evaluation (AF/TE), who serves under the authority and direction of the Secretary of the Air Force (SECAF) and the Chief of Staff of the Air Force (CSAF), in accordance with Headquarters Air Force Mission Directive 1-52 (HAF MD 1-52). In this capacity, the AF/TE:

- Functions as the sole focal point for Air Force T&E policy, guidance, direction, and oversight for the formulation, review, and execution of T&E plans, programs, and budgets.
- Functions as the chief T&E advisor to senior Air Force leadership on T&E processes; including contractor testing, DT&E, OT&E, LFT&E, and the use of modeling and simulation in T&E.

- Functions as the final T&E review authority and signatory for TEMPs prior to Component Acquisition Executive (CAE) and OSD approval and signature.
- Collaborates with requirements sponsors and system developers to improve operational requirements, system development, and the fielding of operationally effective, operationally suitable, safe, and survivable systems.
- Reviews and/or prepares T&E information for timely release to OSD, Congress, and decision-makers.
- Oversees the Air Force T&E infrastructure by determining the adequacy of T&E resources required to support system acquisition activities. Administers various T&E resource processes and chairs or serves on various committees, boards, and groups supporting T&E activities.
- Acts as the single point of entry for the Air Force Foreign Materiel program.
- Manages the Air Force Joint Test & Evaluation program according to DoDI 5010.41, Joint Test and Evaluation (JT&E) program.
- Functions as the certifying authority for T&E personnel in the Acquisition Professional Development Program (APDP) when not delegated to the Major Commands (MAJCOMs).

CH 8–2.3.3 Navy T&E Executive

The Director, Innovation, Test and Evaluation, and Technology Requirements (Office of the Chief of Naval Operations ((OPNAV) N84) serves as the Department of Navy (DON) T&E Executive, as outlined in Secretary of the Navy Instruction (SECNAVINST) 5000.2E (Para 7(g) – page 7). The DON T&E Executive reports to the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and the Principal Military Deputy to the Assistant Secretary of the Navy for Research, Development, and Acquisition (PMD ASN(RDA)), on all matters pertaining to T&E.

The DON T&E Executive supports and advises the Vice Chief of Naval Operations (VCNO) regarding the VCNO's role on the T&E Executive Board of Directors and serves as the Navy representative on the T&E Executive Board of Directors (Executive Secretariat).

The Director, Test and Evaluation and Technology Requirements (N84):

- Approves all Navy TEMPs for the CNO.
- Establishes Navy T&E requirements and promulgates policy, regulation, and procedures governing Navy T&E.
- Acts for CNO in resolving T&E requirements.

CH 8–2.3.4 Operational Test Agencies

This section provides information on the Defense Information Systems Agency (DISA) and the Service's' Operational Test Agencies (OTAs). In accordance with DoDD 5000.01 (Encl. 1, para E1.1.8. – page 6), each Military Department shall establish an independent OTA reporting directly to the Service Chief to plan and conduct operational tests, report results, and provide evaluations of operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality.

CH 8–2.3.4.1 DISA Joint Interoperability Test Command

The Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC) conducts operational testing of information technology and National Security Systems acquired by DISA, other DoD organizations, and non-DoD entities to ensure operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality, and security, in accordance with DoDD 5105.19 (Para 6.1.8.4. – page 6). JITC assists in the preparation of critical operational issues and develops, defines, and publishes measures of operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality, and measures of performance. The division also directs and approves OT&E methods for data collection, reduction, and analysis.

As part of the overall OT&E mission, JITC executes these specific methodologies for determining levels of operational testing appropriate to the risk posed by specific system increments:

- Prepare a risk assessment.
- Determine appropriate level of OT&E.
- Develop an OT&E plan appropriate for the level of test.
- Conduct test activities and prepare a report.
- Provide operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality and security recommendations.

CH 8–2.3.4.2 Army T&E Command

The U.S. Army Test and Evaluation Command (ATEC) is the Army's OTA and consists of the U.S. Army Evaluation Center (AEC), U.S. Army Operational Test Command (OTC), and Test Centers. AEC produces independent comprehensive evaluations and assessments by consolidating all DT, OT, and other credible data so as to provide essential information to decision-makers. Additionally, AEC produces system safety documentation. OTC plans, conducts, and reports on operational tests in order to provide essential information to AEC. ATEC's Test Centers plan, conduct, and report on developmental tests in order to provide essential information to AEC. Army Regulation 73-1 (Para 2 (2-2(d)(7) – page 3) [NOTE: due to authentication controls, you must start from Army ePubs page and search in Publications/Administrative/Army Regulations for AR 73-1.] provides additional information on ATEC responsibilities.

CH 8–2.3.4.3 Air Force Operational T&E Center

The Air Force Operational Test and Evaluation Center (AFOTEC) tests and evaluates new Air Force warfighting capabilities in operationally realistic environments, influencing and informing national resource decisions, in accordance with Air Force Mission Directive 14 (AFMD-14) and Air Force Instruction 99-103 (AFI 99-103) (CH 3.11 – page 28).

CH 8–2.3.4.4 Navy Commander of Operational T&E

The Navy Commander of Operational Test and Evaluation (COMOPTEVFOR) provides an independent and objective evaluation for the operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality of naval aviation; surface; subsurface; command, control, communications, computers, and intelligence (C4I); cryptologic; and space systems in support of DoD and Navy acquisition and fleet introduction decisions, in accordance with SECNAVINST 5000.2E (Para 7(i) – page 8).

CH 8–2.3.4.5 Marine Corps Operational T&E Activity

The Marine Corps Operational Test and Evaluation Activity (MCOTEA) provides operational testing and evaluation for the Marine Corps, and conducts additional testing and evaluation, as required, supporting the Marine Corps mission to man, train, equip, and sustain a force in readiness, in accordance with SECNAVINST 5000.2E (Para 7(i) – page 8).

CH 8–2.3.5 T&E Executive Board of Directors

The Test and Evaluation Executive Board of Directors (BOD) leads development of corporate OSD guidance for T&E infrastructure and configuration management, standards and policy, and investments. The BOD acts as the agent for the Service Vice Chiefs and equivalent Office of the Under Secretary of Defense (OUSD) and Defense Agency representatives with T&E management responsibilities. It consists of the Service T&E executives and equivalent OUSD and Defense Agency representatives with T&E infrastructure management responsibilities.

CH 8–2.4 Program Office T&E Personnel & Support

Management responsibility for an acquisition program's T&E ultimately resides with the PMs. However, the planning, executing, and reporting of T&E involves interactions, support, and engagement from other organizations within OSD, the Services, Defense Agencies, and in some cases, other government agencies, as well as the system contractor(s). In accordance with DoDI 5000.02 (Encl. 4, para 3(e) – page 66, program managers will designate a T&E WIPT (also known as an Integrated Test Team), as soon as practicable after the Materiel Development Decision to support development of T&E strategies and estimates of resource requirements. An early charter for a T&E WIPT proves essential to the success of a T&E program. The Chief Developmental Tester chairs the T&E WIPT. For additional information, consult "DoD Integrated Product and Process Development Handbook" (August, 1998).

The PM, in concert with the user and the T&E community, coordinates DT&E, OT&E, LFT&E, system-of-systems (SoS) performance testing, interoperability testing, cybersecurity testing, reliability growth testing, safety testing, modeling and simulation (M&S), and CBRN survivability activities into an efficient continuum, closely integrated with requirements definition and systems design and development. The PM has responsibility for developing and obtaining final approval of the TEMP, which describes the overall strategy for T&E supporting the program's Acquisition Strategy (AS) and Systems Engineering Plan (SEP); the validated ICD, CDD, or CPD; the Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP); mandatory Enterprise Architecture views; as well as the resources necessary to execute the test program.

For additional information on PM responsibilities, see DoDI 5000.02 (Encl. 2, para 6 – page 55).

CH 8–2.4.1 Chief Developmental Tester

As outlined in 10 USC 1706 (para a), DoDI 5000.02 (Encl. 4, para 3(a) – page 65), and the AT&L Memorandum, "Key Leadership Positions and Qualification Criteria," PMs will designate a Chief Developmental Tester for each MDAP and MAIS program. PMs for MDAP programs shall designate a government test agency as the Lead DT&E Organization, in accordance with DoDI 5000.02 (Encl. 4, para 3(b) – page 91). Further, PMs are to designate a Chief Developmental Tester and Lead DT&E Organization as soon as practicable after program office establishment.

For MDAP and MAIS programs, the Chief Developmental Tester position is filled by a properly qualified member of the Armed Forces or full-time employee of the DoD in a Key Leadership Position (KLP). The Chief Developmental Tester is to occupy a Defense Acquisition Workforce Improvement Act (DAWIA) T&E acquisition-coded position designated as a KLP, and be assigned or matrixed to a single ACAT program. A Chief Developmental Tester is to be designated for all ACAT II programs and below. ACAT II and below Chief Developmental Testers are to occupy a DAWIA T&E Coded position, but are not required to be designated as a KLP.

The Chief Developmental Tester has responsibility for:

- Coordinating the planning, management, and oversight of all DT&E activities for the program.
- Maintaining insight into contractor activities under the program.
- Overseeing the T&E activities of other participating government activities under the program.
- Helping program managers make technically informed, objective judgments about contractor developmental test and evaluation results under the program.
- Chairing the T&E WIPT.

CH 8–2.4.2 Key Leadership Positions

The USD(AT&L) memorandum, "Key Leadership Positions and Qualification Criteria," ensures KLPs are assigned to all MDAP and MAIS (ACAT I and ACAT IA) programs. Mandatory KLPs include the Chief Developmental Tester who, in compliance with the memorandum, is to be designated in the position category associated with the lead function (T&E), and designated to a single ACAT program.

Positions are to be filled by properly qualified members of the Armed Forces or full-time employees of the DoD. KLPs require a significant level of authority commensurate with the responsibility and accountability for acquisition program success. The five factors identified as essential requirements for selection are education, experience, cross-functional competencies, tenure, and currency. Additional functional-specific requirements and preferences for KLPs are located at the DAU iCatalog. These requirements are updated annually by the functional leader for each career field.

CH 8–2.4.3 T&E Working-Level Integrated Product Team

Integrated Product Teams (IPTs) (also known as Integrated Test Teams) serve as an integral part of the DoD acquisition oversight and review process. DoD adopted the use of IPTs as an approach for the review and oversight of the acquisition process. IPTs take advantage of all members' expertise, produce an acceptable product, and facilitate decision-making.

In accordance with DoDI 5000.02 (Encl. 4, para 3(e) – page 66 & Encl. 5, para 4(a) – page 70), the T&E WIPT serves as a defined forum supporting the PM and other program working-level integrated product planning groups on all aspects of a program's T&E efforts and tracks the T&E program in all phases. This effort includes T&E program strategy, design, development, oversight; and the analysis, assessment, and reporting of test results. T&E WIPTs meet, as required, to help the PM resolve test issues. The Chief Developmental Tester ensures the PM establishes and charters a T&E WIPT as soon as practicable after the Materiel Development Decision, thus ensuring involvement in program strategy discussions and plans.

The T&E WIPT will include empowered representatives of test data stakeholders such as systems engineering, DT&E, OT&E, LFT&E, product support, the user, the intelligence community, and applicable certification authorities. The T&E WIPT is chaired by the Chief Developmental Tester and the membership includes, as a minimum, the following representative membership:

- The designated government Lead DT&E Organization.
- The designated Operational Test Agency (OTA).
- Proponent/User.
- Oversight organizations (OSD or Service/Defense Agency Headquarters, depending on whether the program is on oversight).
- Organizations issuing certifications and accreditations based on test data (e.g., Security Control Assessor (SCA), JITC, etc.).
- All evaluating and reporting organizations for the program.
- Organizations that generate test data for the program.
- Organizations requiring T&E data for the program.
- Other supporting or participating test organizations, when appropriate.
- Logistics and training organizations, when appropriate.
- The system contractor, when the contract has been awarded.
- Intelligence/Threat organization.

The T&E WIPT:

- Provides a forum for involvement by all key organizations in the T&E effort.
- Supports the development and tracking of an integrated test program for DT, OT, live fire, and modeling and simulation to support evaluations.
- Supports the development and maintenance of the integrated test schedule.
- Identifies and resolves test issues.
- Documents a TEMP development and coordination schedule as quickly as possible to ensure all interested parties are afforded an opportunity to contribute to TEMP development.
- Explores and facilitates opportunities to conduct Integrated Testing to meet DT/OT objectives.

The PM may form lower level functional working groups that report to the WIPT. These groups focus on specific areas such as integrated test planning; cybersecurity; software T&E; reliability; modeling and simulation development and use; verification, validation, and accreditation (VV&A); and threat support.

CH 8–2.4.4 Lead Developmental T&E Organization

In accordance with DoDI 5000.02 (Encl. 4, para 3(b) – page 91), each MDAP is to be supported by a Lead DT&E Organization. The Lead DT&E Organization is a government test organization and should be independent from the program office, when feasible. The Lead DT&E Organization has responsibility for:

- Providing technical expertise on T&E issues to the Chief Developmental Tester for the program.
- Conducting DT&E activities for the program, as directed by the Chief Developmental Tester.
- Assisting the Chief Developmental Tester in providing oversight of contractors under the program and in reaching technically informed, objective judgments about contractor DT&E results under the program.

For all other programs, a Lead DT&E Organization is used, when feasible, and identified in the CH 8–3.6 Test & Evaluation Master Plan.

CH 8–2.5 Program Engagement

This section provides information on DASD(DT&E) and DOT&E program engagement efforts.

CH 8–2.5.1 DT&E Engagement List

DASD(DT&E) monitors the activities of MDAP and MAIS programs, as well as USD(AT&L) designated special interest programs. In accordance with DoDI 5000.02 (Encl. 4, para 2(e) – page 65), DASD(DT&E) uses the MDAP, MAIS, and AT&L designated special interest lists (active programs and select inactive programs) to identify programs for DT&E oversight.

Access to the USD(AT&L) designated special interest list requires a Defense Acquisition Management Information Retrieval (DAMIR) account (DoD CAC required). Once inside DAMIR, find the “Business Intelligence” link and select Standard Data Queries, then select Program Information, and then select Special Interest Program List, which can then be exported into one of several formats.

For MDAP and MAIS definitions, see DoDI 5000.02 (Encl. 1, Table 1 – page 29).

CH 8–2.5.2 DOT&E Oversight List

Based on DoDI 5000.02 (Encl. 5, para 3 – page 70), the Director, Operational Test and Evaluation (DOT&E) designates programs for OT&E and/or LFT&E oversight, and publishes a DOT&E Oversight List. DOT&E considers all programs for inclusion, regardless of ACAT level, and can add to or delete from the list at any time. DOT&E considerations for inclusion on formal T&E oversight include:

- ACAT level.
- Potential for Joint designation.
- Potential for establishment as an acquisition program (such as Technology Projects identified in DoDI 5000.02 (Encl. 13, para 4(a)(3)(h) – page 100) or a pre-Major Defense Acquisition Program (MDAP)).
- Stage of development or production.
- Potential for DAES reporting.
- Congressional and/or DoD interest.
- Programmatic risk (cost, schedule, or performance).

- Past programmatic history of the developmental command.
- Relationship with other systems as part of a system-of-systems (SoS).
- Technical complexity of system.
- CBRN mission-critical systems.

CH 8–2.6 Program Reporting

This section provides information on the various DASD(DT&E) and DOT&E program reporting requirements.

CH 8–2.6.1 DT&E Program Reporting

DoDI 5000.02 (Tables 2 – 8), summarizes statutory and regulatory reporting requirements, as well as specifying report requirements. The program reports that follow can be found in Table 5, and exceptions to reporting can be found in Table 6 of DoDI 5000.02 (Encl. 1 – page 28).

CH 8–2.6.1.1 Congressional Notification of Conducting DT&E without an Approved TEMP

In accordance with P.L. 112-239, (SEC. 904 para h(3)), the USD(AT&L) notifies Congress not later than 30 days after any decision to conduct DT&E on an MDAP without an approved TEMP in place. The PM prepares and submits the notification to the USD(AT&L). The notification must include:

- A written explanation of the basis for the decision.
- A timeline for getting an approved plan in place.

A copy of the notification is provided to the DOT&E.

CH 8–2.6.1.2 DT&E Exception Reporting

Table 2 identifies the two cases for which Developmental Test and Evaluation (DT&E) submits an annual report to Congress.

Table 2: DT & E Exception Reporting

In accordance with P.L. 112-239 (SEC. 904 para (h(1)(A)) & (B)), the USD(AT&L) submits an annual Report to Congress (from fiscal year 2013 through fiscal year 2018) for the following conditions:	
Case 1	When an MDAP proceeds with implementing a TEMP that includes a developmental test plan disapproved by the DASD(DT&E).
	The Chief Developmental Tester needs to assist the PM to provide DASD(DT&E) the essential information for inclusion in the report. The report includes: ○ A description of the specific aspects of the DT&E plan determined to be inadequate. ○ An explanation of why the program disregarded the DASD(DT&E)'s recommendations. ○ A description of the steps taken to address the concerns of the DASD(DT&E).

In accordance with P.L. 112-239 (SEC. 904 para (h(1)(A)) & (B)), the USD(AT&L) submits an annual Report to Congress (from fiscal year 2013 through fiscal year 2018) for the following conditions:	
Case 2	When an MDAP proceeds to IOT&E following an assessment by DASD(DT&E) that the program is not ready for operational testing.
	The Chief Developmental Tester needs to assist the PM in providing the essential information to the DASD(DT&E) for inclusion in the report. The report includes: ○ An explanation of why the program proceeded to IOT&E despite the DASD(DT&E) findings. ○ A description of the aspects of the TEMP that had to be set aside to enable the program to proceed to IOT&E. ○ A description of how the program addressed the specific areas of concern raised in the assessment of operational test readiness. ○ A statement of whether IOT&E identified any significant shortcomings in the program.

CH 8–2.6.2 DOT&E Reporting

In accordance with 10 USC 2399 (Para a), the Director, Operational Test and Evaluation (DOT&E) provides a Beyond Low-Rate Initial Production (BLRIP) report to the SecDef, USD(AT&L), and congressional defense committees on the adequacy of OT&E conducted for each MDAP), and whether the results of such T&E confirm that the items or components actually tested are operationally effective, operationally suitable, and survivable (including cybersecurity) for combat. Additionally, in accordance with DoDI 5000.02 (Encl. 1, Table 2 – pages 36), DOT&E completes the LFT&E report requirement for submission to the congressional defense committees, SecDef, and USD(AT&L) before the system may proceed to Full-Rate Production (FRP). For purposes of compliance with completion of IOT&E, the PM ensures the system under test reflects production-configuration or production-representative systems, preferably LRIP articles.

CH 8–2.7 TEMP Overview

The Test and Evaluation Master Plan (TEMP) is a signed contract among DOT&E, the DASD(DT&E), senior DoD Component leadership, the lead OTA, and the PM describing an acquisition program's T&E strategy and planned T&E activities over a program's life cycle, in accordance with DoDI 5000.02 (Encl. 5, para 5(a) – page 70). It serves as an executive summary and provides a developmental and operational evaluation framework to identify key data that will contribute to assessing the system's progress toward achieving requirements. It also is used as a guide when developing detailed T&E plans and documents, as well as schedule and resource implications associated with the T&E program. The program manager will use the TEMP as the primary planning and management tool for all test activities starting at Milestone A.

The TEMP includes a strategy for T&E and begins with a review and understanding of the threat and the requirements. The purpose of a T&E program is to characterize system capabilities across the intended operational conditions, verify that testable requirements are met or not met, and inform decision-makers. Program managers devise a T&E strategy generating the knowledge necessary for the acquisition, programmatic, operational, technical, and life-cycle support decisions of a program. Forming an effective T&E strategy requires careful analysis to determine the appropriate scope and depth of evaluations to be completed. This approach to T&E strategy development is to plan for the evaluation before testing, execute the test program, and conduct the evaluation as test data become available. This creates an environment where the evaluation guides the formulation of test objectives, configurations, conditions, data requirements, and analysis to develop information in support of the decision-making process.

For more information, go to DAG CH 8.3.6., Test & Evaluation Master Plan.

CH 8–3. Guidance

In accordance with 10 USC 139, 2399, 2400, and 2366 as well as DoDI 5134.17 and DoDD 5141.02, DoD employs three formal types of T&E (DT, OT, and LFT&E). Within these broad categories, the Military Departments and Defense Agencies have their own directives, guidance, organizations, T&E resources, ranges, and facilities specific to their needs.

This section provides the responsibilities and distinguishing features of each type of T&E. In addition, this section provides information on Integrated Testing and which programs should conduct such testing whenever feasible, to permit all stakeholders to use the same data in support of their respective evaluations.

The TRMC, in accordance with 10 USC 196 (Para c(1)(A)(i)), oversees the Major Range and Test Facility Base (MRTFB), and ensures availability of capabilities to support T&E.

Although the words *test* and *evaluation* are sometimes used interchangeably, they are two different concepts:

- Testing is a program or procedure designed to measure characteristics of an entity under identified conditions.
- Evaluation is the determination and substantiated judgment of risk associated with the significance, worth, or quality of capabilities or limitations of an entity, components, integrated system, or participant in a system-of-systems, using criteria established by systems engineers or users.

CH 8–3.1 Developmental T&E

Developmental Test and Evaluation (DT&E) is the disciplined process of generating substantiated knowledge on the capabilities and limitations of systems, subsystems, components, software, and materiel. This knowledge is used to inform decision-makers on risks in acquisition, programmatic, technical, and operational decisions throughout the acquisition life cycle. DT&E assesses maturity of technologies, system design, readiness for production, acceptance of government ownership of systems, readiness to participate in distributed and operational T&E, and sustainment in accordance with DoDI 5000.02 (Encl. 4, para 2(e) – page 65).

Both test and evaluation are necessary to gain value from a DT&E effort. In the context of DT&E, an entity can be a technology, process, materiel, software modules, components, subsystems, systems, and system-of-systems. Identified conditions refer to test conditions that are controlled, uncontrolled, measured, or not measured. Developmental evaluations are accomplished using criteria derived from various sources. The most common sources are the mission sets from the Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP), the capability gaps, user requirements specified in the capabilities documents (Initial Capabilities Document (ICD), Capability Development Document (CDD), Capability Production Document (CPD)), Critical Operational Issues (COIs), and Critical Operational Issues and Criteria (COIC), the design measures contained in the technical requirements documents (TRD), and contractual performance specifications. One set of tests can result in multiple developmental evaluations.

A DT&E program will:

- Verify achievement of critical technical parameters and the ability to achieve key performance parameters, and assess progress toward achievement of critical operational issues.
- Assess the system's ability to achieve the thresholds prescribed in the capabilities documents.

- Provide data to the program manager to enable root cause determination and to identify corrective actions.
- Validate system functionality.
- Provide information for cost, performance, and schedule tradeoffs.
- Assess system specification compliance.
- Report on program progress to plan for reliability growth and to assess reliability and maintainability to performance for use during key reviews.
- Identify system capabilities, limitations, and deficiencies.
- Include T&E activities to detect cyber vulnerabilities within custom and commodity hardware and software.
- Assess system safety.
- Assess compatibility with legacy systems.
- Stress the system within the intended operationally relevant mission environment.
- Support cybersecurity assessments and authorization, including Risk Management Framework security controls.
- Support the interoperability certification process.
- Document achievement of contractual technical performance, and verify incremental improvements and system corrective actions.
- Assess entry criteria for Initial Operational Test and Evaluation (IOT&E) and Follow-On Operational Test and Evaluation.
- Provide DT&E data to validate parameters in models and simulations.
- Assess the maturity of the chosen integrated technologies.

Other areas DT&E contributes to include:

- Data collection, migration, management, and archiving.
- Software functionality validation.
- Cybersecurity.
- Interoperability.
- Interface design and management.
- Integration.
- Modeling and simulation verification, validation, and accreditation.
- Environmental compliance and impact.
- Reliability.
- Logistics Demonstration.

CH 8–3.1.1 Program Planning

The Test and Evaluation Master Plan (TEMP) is the primary planning and management tool for the integrated test program, in accordance with DoDI 5000.02 (Encl. 4, para 5 – page 66). At a minimum, the following documents (unless MDA waiver is obtained) are used to support development of the TEMP:

- JCIDS documents (ICD, CDD, CPD).
- Critical Operational Issues (COIs) and Critical Operational Issue Criteria (COIC).
- Analysis of Alternatives (AoA).
- System Threat Assessment Report (STAR) (Note: The Validated Online Life-cycle Threat (VOLT) is being developed to replace the STAR.).
- Acquisition Strategy (AS).
- Systems Engineering Plan (SEP).
- Program Protection Plan (PPP).
- Cybersecurity Strategy.

- Security Plan.
- Security Assessment Plan.
- Information Support Plan (ISP).
- Acquisition Program Baseline (APB).
- Cost Analysis Requirements Description (CARD).
- Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP).

CH 8–3.1.2 Evaluation of Developmental Test Adequacy

DT&E provides feedback to the PMs and decision-makers to inform decision-making throughout the acquisition cycle. The PM uses the TEMP as the primary planning and management tool for the integrated test program. The TEMP should describe a logical DT&E strategy, including: (1) decisions to be informed by the DT&E information, (2) evaluations to inform those decisions, (3) test and modeling and simulation events to be conducted to generate the data for the evaluation, and (4) resources to be used and schedules to be followed to execute T&E events. A comprehensive DT&E program generates the key data used to evaluate technologies, components, subsystems, interoperability, cybersecurity, and reliability capabilities. In accordance with DoDI 5000.02 (Encl. 4, para 5(a)(6) – page 67), the TEMP includes a developmental evaluation framework that shows the correlation/mapping between decisions, capabilities to be evaluated, measures to be used to quantify the capabilities, and test and modeling and simulation events.

CH 8–3.2 Operational T&E

Service and Defense Agency OTAs have the responsibility for planning, conducting, and assessing the results of OT&E. OT&E is used to determine the operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality of a system when operated under realistic operational conditions, including Joint combat operations and system-of-systems concept of employment; evaluates whether threshold requirements in the approved JCIDS documents and critical operational issues have been satisfied; assesses impacts to combat operations; and provides additional information on the system's operational capabilities, limitations, and deficiencies.

The OTAs and DOT&E have a requirement to address operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality in their evaluations. This evaluation is a mission capability assessment influenced more by the combatant commander/force commander's operational plans and concept of operations than specific system requirements and takes into account all associated systems (an end to end, system-of-systems evaluation) involved in the kill chain. In some instances, programs have successfully demonstrated their Key Performance Parameters (KPPs), Key System Attributes (KSAs), and Critical Technical Parameters (CTPs), but were not evaluated as Operationally Effective and/or Operationally Suitable by DOT&E. Conversely, some programs were evaluated as Operationally Effective and/or Operationally Suitable by DOT&E even though they did not successfully achieve one or more KPPs/KSAs/CTPs. Program managers work closely with the OTA and DOT&E to help determine the assessment of mission capabilities in OT; evaluations include both an assessment of KPPs/KSAs/CTPs, and an assessment of mission effectiveness with a focus on the intended operating environments, threats, concept of operations, critical operational issues, and the concept of employment across the operational envelope. In the memorandum, "Reporting of Operational Test and Evaluation (OT&E) Results," the DOT&E states:

- The data used for evaluation are appropriately called measures of effectiveness, because they measure the military effect (mission accomplishment) that comes from the use of the system in its expected environment. This statement of policy precludes measuring operational effectiveness, operational suitability, and survivability (including cybersecurity), or lethality solely on the basis of system-particular performance parameters.
- ". . . "performance attributes" (sic) are often what the program manager is required to deliver….they are not the military effect or measure of operational effectiveness required for achieving the primary purpose" of a mission capability.

- "It is therefore unacceptable in evaluating and reporting operational effectiveness, operational suitability, and survivability (including cybersecurity), or lethality, to parse requirements and narrow the definition of mission accomplishment so that MOP are confused with MOE."

OTAs have a responsibility for early and continued involvement in a system's test program. OTAs conduct EOAs during the Technology Maturation and Risk Reduction (TMRR) phase and OAs during Engineering and Manufacturing Development (EMD) phase. OTAs are also involved in reviewing Capabilities Documents to assess measurability, testability, and operational relevancy of requirements in the JCIDS documents (i.e., Capability Development Document (CDD) and Capability Production Document (CPD)). OTAs' primary responsibilities include the assessment of test adequacy and the evaluation of a system's operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality, or operational security completed in IOT&E and, when necessary, Follow-on Operational Test and Evaluation (FOT&E).

General guidelines for the conduct of OT&E include:

- For dedicated IOT&E, typical users operate and maintain the system under test conditions simulating combat and peacetime operations.
- OT&E uses the most current threats or threat representations to simulate actual threat performance and assess operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality of the system in expected operating environments. Threat representations are validated by the DoD Components using Defense Intelligence Agency (DIA), the DoD Component intelligence agency, or Service intelligence organization approved and validated threat data that describe threat characteristics and performance. DOT&E approves validation reports for threat surrogate systems planned to be used to support OT&E for OSD oversight programs.
- Conducting cybersecurity T&E for all weapon, information, and Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems depending on external information sources, or providing information to other DoD (or non-DoD) systems. Cybersecurity assessments will include both IP and non-IP (1553 bus, data links, etc.).
- Persons employed by the contractor for the system under development may only participate in the OT&E of systems to the extent the PM planned for their involvement in the operation, maintenance, and other support of the system in peacetime or when deployed in combat.
- Testing production representative systems includes any system accurately representing its final configuration, using mature and stable hardware and software that accurately mirrors the production configuration, but not necessarily produced on a final production line.
- OTAs assume configuration control of test articles (hardware, software, and firmware) prior to OT&E.

CH 8–3.2.1 Evaluation of Operational Test Adequacy

Operational Test adequacy encompasses both test planning and test execution. Operational testing requires the testing of systems under test conditions simulating combat and peacetime operations. In addition, the system must be production-representative, and typical operators must operate and maintain the system. An adequate evaluation requires sufficient testing in this environment to draw conclusions. Considerations include:

- Realistic combat-like conditions
  - Equipment and personnel under realistic stress and operations tempo.
  - Threat representative forces.
  - End-to-end mission testing.

    - Realistic combat tactics for friendly and enemy.
    - Operationally realistic environment, targets, countermeasures.
    - Includes all interfacing systems.
- Production representative system for IOT&E
    - Articles off production line preferred.
    - Production representative materials and process.
    - Representative hardware and software.
    - Representative logistics, maintenance, and training manuals.
- Adequate resources
    - Sample size and test duration.
    - Size of test unit for friendly and threat surrogate forces, including unique threat equipment.
    - Threat portrayal.
    - Data collection systems and personnel.
- Representative typical users
    - Properly trained personnel, crews, and unit.
    - Typical support personnel and support package.
    - Missions given to units (friendly and hostile).
- System is substantially used to support the mission.
- Collected data are sufficiently complete and accurate.

For more information, see the TEMP Guide.

CH 8–3.2.2 Evaluation of Operational Effectiveness

DoD defines operational effectiveness as the overall degree of mission accomplishment of a system when used by representative personnel in the environment(s) planned or expected for operational employment of the system as well as against or in the presence of realistic and representative threats, including cyber threats. Effectiveness determinations are made considering organization, training, doctrine, tactics, survivability or operational security, vulnerability, and threat.

The evaluation of operational effectiveness is linked to mission accomplishment within the context of the Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP)/Employment. Effectiveness determinations are not limited solely to the evaluation of KPPs, but should also consider how the system's performance varies over the variety of operational conditions and against the variety of threats that the user would encounter when employing the system. Effectiveness determinations might also include a comparison of mission capability to legacy systems, if appropriate, and necessary data are available or are collected to enable such assessments. Early planning for the evaluation considers any special test requirements, such as the need for large test areas or ranges or supporting forces, requirements for threat systems or simulators, modeling test beds, new instrumentation, or other unique support requirements.

For weapon systems, integrate LFT&E of system lethality into the evaluation of weapon system effectiveness. For example, operational testing could identify likely shot lines, hit points, burst points, or miss distances, providing a context for LFT&E lethality assessments. Fuse performance, as determined under DT&E, can provide information for both OT&E and LFT&E.

CH 8–3.2.3 Evaluation of Operational Suitability

Operational suitability defines the degree to which a system is satisfactorily placed and operated in field use, with consideration given to reliability, availability, compatibility, transportability, interoperability,

wartime usage rates, maintainability, safety, human factors, manpower supportability, logistics supportability, documentation, environmental effects, and training infrastructure requirements.

Early planning for the operational suitability evaluation includes any special needs for the number of operating hours, environmental testing, maintenance demonstrations, testing profiles, usability of DT&E data, or other unique test requirements.

Operational suitability is evaluated in a mission context to provide meaningful results. Determinations of reliability and availability must be based on data from system use under operationally realistic system loading while conducting mission operations by field users in all environments and planned operating conditions. Similarly, maintaining a required operational tempo over an extended period while conducting realistic missions gives insight into the interactions of various suitability factors.

Suitability determinations consider how system reliability and availability are affected by different operating environments and conditions and, if appropriate, assess wear-out effects. The ability of the user to set up and employ the system, as well as the complexity of user interfaces and the adequacy of training, are components of the suitability determination. Logistics supply chains and the impacts to operational availability are assessed to the extent possible during OT&E.

Software-intensive systems and hybrid systems' suitability assessment includes the availability, representativeness, and adequacy of their maintenance test environments and regression testing procedures. The ability to reproduce failures observed in the actual system and patching process of the maintenance environment are components of the system's suitability determination.

CH 8–3.2.4 Evaluation of Survivability & Cybersecurity

Survivability defines the degree to which a system can operate in the presence of threats, avoid detection by threats, the extent of damage and ability to maintain operations following engagement by threat weapons, and recover from threat weapon effects. These threats are to include both the kinetic and cyber domains. Survivability and cybersecurity include the elements of susceptibility, vulnerability, and recoverability. As such, survivability and cybersecurity act as an important contributor to operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality. All systems under OT&E oversight receive a survivability and cybersecurity assessment if exposed to cyber or kinetic threat weapons in a combat environment or to combat-induced conditions that may degrade capabilities, regardless of designation for LFT&E oversight. For example, unmanned vehicles may not have a requirement to undergo survivability LFT&E under 10 USC 2366, but receive an assessment for survivability. The assessment may identify issues needing to be addressed through testing.

The purpose of cybersecurity operational test and evaluation is to evaluate the ability of a unit equipped with a system to support assigned missions in the expected operational environment. The system is considered to encompass hardware, software, user operators, maintainers, and the training of Tactics, Techniques, and Procedures used to carry out the Concept of Operations. The operational environment includes other systems that exchange information with the system under test (system-of-systems, including the network environment), end users, administrators and cyber defenders, as well as representative cyber threats. For more information on cybersecurity testing, see DAG CH 8.3.7.5., Cybersecurity.

Integrate DT&E, OT&E, and LFT&E strategies to ensure the consistent assessment of the full spectrum of system survivability and cybersecurity. The Critical Operational Issue (COIs) include any issues that need to be addressed in the OT&E evaluation of survivability and cybersecurity. In accordance with 10 USC 2366, systems under LFT&E oversight must address personnel survivability and integrate it into the overall system evaluation of survivability and cybersecurity conducted under OT&E.

Generally, LFT&E addresses vulnerability and recoverability while OT&E addresses susceptibility, but areas of overlap exist. The evaluation of LFT&E results require realistic hit distributions. The OT&E evaluation of susceptibility might identify realistic hit distributions of likely threats, hit/burst points, and

representative shot lines providing a context for LFT&E vulnerability assessments. DT&E and OT&E testing of susceptibility may provide other LFT&E insights, such as information on signatures, employment of countermeasures, and tactics used for evasion of threat weapons. Similarly, LFT&E tests, such as Total Ship Survivability trials, may provide OT&E evaluators with demonstrations of operability and suitability in a combat environment.

Recoverability addresses the consequences of system damage. Following combat damage, recoverability is the ability to take emergency action to prevent loss of the system, to reduce personnel casualties, or to regain weapon system combat mission capabilities. LFT&E typically addresses recoverability; however, both OT&E and LFT&E have an interest in tests relating to recoverability from combat damage or from peacetime accidents.

LFT&E conducts Real Time Casualty Assessment (RTCA) during IOT&E to ensure assumptions supporting the RTCA remain consistent with LFT&E results.

CH 8–3.2.5 Live Fire Test & Evaluation

This section provides information on Live Fire Test and Evaluation (LFT&E) objectives, evaluation of covered systems, early LFT&E, the waiver process, and personnel survivability, in accordance with DoDI 5000.02 (Encl. 5, para 11 – page 74).

CH 8–3.2.5.1 Live Fire Test & Evaluation Objectives

PMs plan and execute an LFT&E program if DOT&E designates their program for LFT&E oversight, in accordance with DoDI 5000.02 (Encl. 5, para 9 – page 74). LFT&E program objectives provide a timely evaluation of the vulnerability/lethality of a system as it progresses through design and development prior to full-rate production. In particular, LFT&E programs:

- Provide information to decision-makers on potential user casualties, vulnerabilities, and lethality, taking into equal consideration susceptibility to attack and combat performance of the system.
- Ensure testing of the system under realistic combat conditions includes knowledge of user casualties and system vulnerabilities or lethality.
- Allow for correction in design or employment of any design deficiency identified by T&E before proceeding beyond LRIP.
- Assess recoverability from battle damage and battle damage repair capabilities and issues.

The PM includes planning factors in the structure and schedule for the LFT&E Strategy to accommodate and incorporate any design changes resulting from testing and analysis before proceeding beyond LRIP.

CH 8–3.2.5.2 Covered Systems

A covered system defines a system that DOT&E, acting for the SecDef, designates for LFT&E oversight, in accordance with DoDI 5000.02 (Encl. 5, para 9 – page 74). These systems include, but are not limited to, the following categories:

- Any major system within the meaning of that term in 10 USC 2302 (Para 5), including user-occupied systems, and designed to provide some degree of protection to its occupants in combat.
- A conventional munitions program or missile program; or a conventional munitions program planning to acquire more than 1,000,000 rounds (regardless of major system status).
- A modification to a covered system likely to significantly affect the survivability or lethality of such a system.

CH 8–3.2.5.3 Early Live Fire Test & Evaluation

In accordance with DoDI 5000.02 (Encl. 5, para 11(a)(2) – page 75), conducting LFT&E events early in a program's life cycle allows time to correct any design deficiency demonstrated by T&E when impacts to program costs and schedule are least. Where appropriate, the PM may correct the design or recommend adjusting the employment of the covered system before proceeding beyond LRIP. LFT&E typically includes testing at the component, subassembly, and subsystem level; and may also draw upon design analyses, modeling and simulation, combat data, and related sources such as analyses of safety and mishap data. As a standard practice, this occurs regardless of whether the LFT&E program culminates with Full-Up, System-Level (FUSL) testing or not.

CH 8–3.2.5.4 Full-Up, System-Level Testing

10 USC 2366 (Para b) defines Full-Up, System-Level Testing as testing that fully satisfies the statutory requirement for "realistic survivability" or "realistic lethality testing." The criteria for FUSL testing differ somewhat based on the type of testing: survivability, operational security, or lethality. The following are types of FUSL testing:

- Vulnerability testing is conducted using munitions likely to be encountered in combat on a complete system loaded or equipped with all the dangerous materials that normally would be on board in combat (including flammables and explosives), and with all critical subsystems operating that could make a difference in determining the test outcome.
- Lethality testing of production-representative munitions or missiles, for which the target is representative of the class of systems that includes the threat; and the target and test conditions are sufficiently realistic to demonstrate the lethality effects the weapon is designed to produce.

CH 8–3.2.5.5 Full-Up, System-Level Testing Waiver Process

In accordance with 10 USC 2366 (Para c), an LFT&E program includes FUSL testing unless granted a waiver. When required, a waiver package is submitted to the appropriate congressional defense committees prior to Milestone B; or, in the case of a system or program initiated at Milestone B, as soon as practicable after Milestone B; or, if initiated at Milestone C, as soon as practicable after Milestone C. Typically, this occurs at the time of TEMP approval.

The waiver package includes certification by the Defense Acquisition Executive (DAE) to Congress that FUSL testing would prove unreasonably expensive and impractical. In accordance with DoDI 5000.02 (Encl. 1, Table 6 – page 43), it also includes a DOT&E-approved alternative plan for conducting LFT&E in the absence of FUSL testing. Typically, the alternative plan reflects the LFT&E strategy in the TEMP. This alternative plan includes LFT&E of components, subassemblies, or subsystems and, as appropriate, additional design analyses, modeling and simulation, and combat data analyses.

CH 8–3.2.5.6 Personnel Survivability

LFT&E has a statutory requirement to address personnel survivability (i.e., force protection) for covered systems as part of "realistic survivability testing." In 10 USC 2366 (Para e(3)), the term realistic survivability testing means "testing for vulnerability of the system in combat by firing munitions likely to be encountered in combat (or munitions with a capability similar to such munitions" at the system configured for combat. The primary emphasis is on testing vulnerability with respect to potential user casualties and taking into equal consideration the system's susceptibility to attack as well as the combat performance of the system. Personnel survivability should be addressed through dedicated measures of evaluation, such as "expected casualties" supported by specific details on the type and severity of injury, as well as the potential operational impact of such casualties on the ability of the platform to accomplish its mission after a threat engagement, when appropriate. Personnel survivability must also be addressed even in cases where the platform cannot survive.

CH 8–3.3 Integrated Testing

Integrated testing is a concept that capitalizes on the idea that test events can be planned and executed to provide data for both developmental and operational evaluations from the same events. DoDI 5000.02 (Encl. 5, para 11(a)(4) – page 75) defines Integrated Testing as the collaborative planning and collaborative execution of test phases and events to provide shared data in support of independent analysis, evaluation, and reporting by all stakeholders, particularly developmental (both contractor and government), and operational T&E communities. It requires the active participation of the lead OTA in planning the integrated tests with the program office so that the operational objectives are understood, the testing is conducted in an operationally realistic manner, and the resultant data are relevant for use in operational evaluations. The integrated testing approach is documented in the program TEMP. The data pedigree (test conditions and methodologies) are coordinated with the stakeholders prior to execution of the test event.

Integrated testing goals include:

- Conducting a seamless test program producing credible qualitative and quantitative data useful to all evaluators.
- Allowing for the sharing of test events where a single test point or mission can provide data to satisfy multiple objectives without compromising either the developmental or operational test objectives.
- Attaining synergy of effort among all T&E stakeholders including contractor, government developmental and operational representatives, interoperability, cybersecurity, and certification testing in order to maximize use of available test resources and infrastructure.

Integrated testing serves as an implementation concept for test design, not as a new type of T&E. Programs intentionally design integrated testing into the earliest program strategies, plans, documentation, and test plans, preferably starting before Milestone A. Developing and adopting integrated testing strategies early in the process increases the opportunities and benefits. If done correctly, integrated testing provides greater opportunity for early identification of system design improvements, and may even change the course of system development during EMD. Integrated testing is generally more appropriate once the system design has stabilized and the concept of operations is understood. Integrated testing may reduce the scope and number of T&E resources needed in OT&E, if no deficiencies are uncovered and no further design changes are made. However, integrated testing does not replace or eliminate the need for dedicated IOT&E, as required by 10 USC 2399 and DoDI 5000.02 (Encl. 5, para 5(c)(2) – page 71).

Integrated Testing Principles

- While the idea of integrated testing may be well understood ***in theory***, critical implementation requires an understanding of a few basic principles:
  - The integrated testing approach is documented within the TEMP.
  - Data pedigrees are coordinated with stakeholders prior to the start of the test event.
  - Integrated testing is intentionally designed into a program's strategy for T&E.
  - Common T&E parameters, methodologies, and terminology are agreed upon early within the T&E planning.
  - Integrated testing does not replace a dedicated IOT&E.
  - The T&E data are tailored to evaluation requirements.

It is critical that all stakeholders understand the scope of the evaluations required to assess development, design, risks, maturity of the system, the operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality. Up front, define the end state for evaluations, and then develop an integrated test approach that generates the data required to conduct separate evaluations.

For successful integrated testing, understanding and maintaining the pedigree of the data proves vital. The pedigree of the data refers to accurately documenting the configuration of the test asset and the actual test conditions under which each element of test data was obtained. The pedigree of the data indicates whether the test configuration represented operationally realistic or representative conditions. The T&E WIPT plays an important role in maintaining the data pedigree within the integrated test process for a program.

For integrated test results to count for operational testing on DOT&E Oversight List programs, the lead OTA must develop a plan for the integrated test to be approved by DOT&E before the start of testing that, at a minimum, details the required test realism and conditions, operational test objectives, operational test metrics, production representative test articles, and data collection requirements, in accordance with DoDI 5000.02 (Encl. 5, para 11(a)(4)(b) – page 75). Data collected outside an approved operational test plan or major live-fire test plan can be used for a DOT&E operational or live fire evaluation if the data are approved by DOT&E. Depending on circumstances, DOT&E approval will not necessarily be possible in the TEMP and may require some other documentation. Data approval will be based on understanding the realism of the test scenario(s) used and the pedigree of the data. The data in question typically come from operational exercises, certification events, and developmental test events in operationally relevant environments. Data approval is coordinated with the Lead DT&E Organization and DOT&E prior to the start of testing. When advanced coordination is not possible, the Lead DT&E Organization facilitates data reuse (in a DOT&E assessment or evaluation) through independent documentation of the test data pedigree (test conditions and methodologies). For non-oversight programs, the OTA will determine what integrated test results will count for operational testing.

In accordance with DoDI 5000.02 (Encl. 4, para 2(c) – page 65), integrated testing provides shared data in support of independent analyses for all T&E stakeholders. Integrated testing must allow for and support separate and independent OT&E, in accordance with 10 USC 2399 and DoDI 5000.02 (Encl. 5, para 11(a)(4)(b)) – page 75).

CH 8–3.4 Test Risk Management & Mitigation

Risk management and mitigation is an important part of every acquisition program. The *Defense Acquisition Guide,* Chapters 1 and 3, address program risk management. The Risk Management Guide for DoD Acquisition provides more detailed information.

In accordance with DoDI 5000.02 (Encl. 5, para 6(c)(2)(a) – page 72), potential test-related risks include, but are not limited to:

- Program delays that may compress available test execution time.
- Test assets that may arrive late or have unresolved deficiencies.
- Availability of any other planned resources (facilities, personnel, etc.).
- An overly optimistic test schedule that prevents timely delivery of information.
- Environment, Safety, and Occupational Health (ESOH) risk management.

Nearly any assumption the PM makes regarding the test program may constitute a potential risk. Test limitations and constraints also pose potential risks. Early T&E WIPT meetings include discussions on risk identification and mitigation.

The T&E WIPT also assesses the severity of the risk according to the program's risk management plan. Normally, medium and high-risk items are elevated to the program's risk management board for action, while low risks remain with the Chief Developmental Tester and the T&E WIPT for management. A formal risk mitigation plan is developed for medium and high risks, and the mitigation steps are included in the program integrated master schedule. Again, following the program's risk management plan for guidance is the best course of action.

Medium and high test risks known at the time of TEMP development are included in the TEMP, rather than a generic description of a risk management process. Risks may change over time, and the T&E WIPT regularly reviews test risks and actively works with the program's risk management board to keep test risks current.

For more information, DAG CH 8.3.24, Safety Reviews, serves as a reference source.

CH 8–3.5 Documentation Used in T&E

T&E personnel advise and engage in the development, review, and use of the following documentation from the outset of each development and acquisition program to ensure expectations and risk assessments remain realistic. These documents are used in development of theTEMP. In accordance with DoDI 5000.02 (Encl. 4, para 6(c) – page 69), the acquisition chain of command will have full and prompt access to all relevant documentation.

To assist in that effort, DASD(DT&E) and DOT&E coordinated with Defense Acquisition University (DAU) to provide a location to house relevant T&E Policy & Guidance documents in one place. The DAU Acquisition Community Connection Test & Evaluation Community of Practice (T&E CoP) (DoD CAC login required) houses the relevant documents. T&E definitions in this chapter are found in the Glossary of Defense Acquisition Acronyms and Terms.

For more information on specific documents, refer to the Milestone Document Identification (MDID) website. The MDID provides a definition of the document, any notes on statutory and/or regulatory requirements, source documents for the specific document, and (if applicable) the approval authority. The MDID allows users to filter by program type, life-cycle event, source, and keyword.

CH 8–3.5.1 Joint Capabilities Integration & Development System

Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3170.01I, Joint Capabilities Integration and Development System, establishes the Joint Capabilities Integration and Development System (JCIDS) process. The JCIDS process is a capabilities-based approach to requirements generation. The process is used by the Joint Requirements Oversight Council (JROC) to fulfill its advisory responsibilities outlined in 10 USC 181 (Para b) to the Chairman of the Joint Chiefs of Staff in identifying, assessing, validating, and prioritizing Joint military capability requirements.

The JCIDS provides a transparent process, allowing the JROC to balance Joint equities and make informed decisions on validation and prioritization of capability requirements. Outputs of the JCIDS process drive the Defense Acquisition System because all acquisition programs respond to validated Capability requirements.

The JCIDS process is tailorable and operates in an iterative manner. The initial capability requirements documents drive the early acquisition process, and the early acquisition process drives updates to capability requirements documents related to specific materiel and non-materiel capability solutions to be pursued. The updated capability requirements documents then drive the development, procurement, and fielding of materiel and non-materiel solutions, satisfying the capability requirements and closing associated capability gaps.

The JCIDS documents serve as a means for sponsors to submit capability requirements and capability gaps identified via established processes, along with other relevant information, for review and validation. The three Capability Requirements documents interacting with the acquisition process are typically called the Initial Capabilities Document (ICD), Capability Development Document (CDD), and Capability Production Document (CPD).

The JCIDS Manual complements CJCSI 3170.01I. It serves as a "living" document with updates incorporated as directed by the JROC. In accordance with the JCIDS Manual, Enclosure B:

- An ICD specifies one or more new capability requirements and associated capability gaps, which represent unacceptable operational risk if left unmitigated. The ICD also documents the intent to partially or wholly address identified capability gap(s) with a non-materiel solution, materiel solution, or some combination of the two. The ICD is the most common starting point for new capability requirements. The validated ICD is a critical entry criterion for the MDD, and guides the sponsor activities during the Materiel Solution Analysis (MSA) phase of acquisition, assessment of potential materiel solutions through an AoA, or similar studies, identifies associated Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities-Policy (DOTmLPF-P) changes, and guides development of other acquisition information required for the Milestone (MS) A review.
- A validated CDD is a critical entry criterion for the development RFP release decision and MS B decision points, and guides the Sponsor in activities during the Engineering and Manufacturing Development (EMD) phase of acquisition. The validated CDD is a key factor in the MDA decision to initiate an acquisition program at MS B. In cases where MS B is not required, but an EMD phase of acquisition will be conducted, the CDD shall be validated ahead of the release of the RFP for the EMD phase of acquisition or the beginning of the EMD phase of acquisition, whichever comes first.
- A CPD provides authoritative, testable capability requirements, in terms of KPPs, KSAs, and additional performance attributes, for the Production and Deployment (P&D) phase of an acquisition program, and is an entrance criteria item necessary for each MS C acquisition decision. The CPD describes the actual performance of a capability solution delivering the required capability, if the system does not meet the threshold levels for the KPPs, or if the cost, schedule, or procurement quantities proposed have been changed since the CDD, the validation authority assesses whether or not the capability solution remains operationally acceptable. The validated CPD is a critical entry criterion for the MS C, and guides the Sponsor in activities during the P&D phase of acquisition. The validated CPD is a key factor in the MDA decision to initiate production of the capability solution at MS C. In cases where MS C is not required, the CPD shall be validated ahead of the release of the RFP for the P&D phase of acquisition or the beginning of the P&D phase of acquisition, whichever comes first.

The CDD and CPD identify the attributes contributing most significantly to the desired operational capability in threshold/objective format. These documents should present each attribute in terms of parameters that are traceable to their associated operational context, and are measurable, testable, and support efficient and effective T&E.

- When appropriate, the attribute includes any unique operating environments for the system. If the capability in a CDD/CPD is part of a system-of-system (SoS) solution, the attributes for the SoS level of performance are described and any unique attributes for each of the constituent systems.
- Other compatibility and interoperability attributes (e.g., databases, fuel, transportability, and ammunition) might need identification to ensure a capability's effectiveness.

The JCIDS process derives and documents performance attributes from analysis supporting the Capabilities-Based Assessment (CBA) and the Analysis of Alternatives (AoA). The CBA, AoA, Measures of Performance (MOPs), Measures of Effectiveness (MOEs), and Measures of Suitability (MOS) remain essential analyses and measures needed for evaluation of those performance attributes.

Test and evaluation personnel primarily assess the testability, measurability, and achievability, clarity of the capabilities required in the documents and provide that assessment to the PM and Chief Engineer. The basic assessment determines the measurability of the capability. Words such as "enhanced," "full spectrum," "unprecedented," "commander's intent," etc., are difficult to measure.

The tester also considers the cost of testing the requirements. The test organization works with the lead system engineer to identify extremely high cost requirements and with the cost estimators to develop alternatives, with modest changes to the requirements, which might yield substantial cost savings.

Together, they request the applicable capability requirements validation authority to reevaluate these original requirements. KPPs and KSAs deserve special attention since they are included in the TEMP.

In accordance with DoDD 5141.02 (Para 4(o) – page 3), the D,OT&E assists the Chairman of the Joint Chiefs of Staff in efforts to ensure the expected Joint operational mission environment, mission-level MOEs, and KPPs are specified in JCIDS documents in verifiable terms through testing or analysis.

Refer to the JCIDS Manual for more information on JCIDS.

CH 8–3.5.2 Analysis of Alternatives

The Analysis of Alternatives (AoA) is an analysis that assesses potential materiel solutions that could satisfy validated capability requirement(s) documented in the ICD, and supports a decision on the most cost-effective solution to meeting the validated capability requirement(s). In developing feasible alternatives, the AoA identifies a wide range of solutions having a reasonable likelihood of providing the needed capability.

AoAs provide a foundation for the development of documents at the milestones, starting at Milestone A. The AoA is used when developing the T&E strategy for the preferred solution(s). The following are some areas in the AoA for the Chief Developmental Tester to consider when developing the T&E strategy:

- Scenarios, threats, environment, constraints and assumptions, timeframe, and excursions.
- Description of alternatives, non-viable alternatives, operations concepts, and support concepts.
- Mission tasks, MOE, MOP, effectiveness analysis, effective methodology, and effectiveness sensitivity analysis.
- Operational risk assessment.
- Technology/manufacturing risk assessment.
- Current/proposed schedules, designs, suppliers, operational employments, resources, dependencies, etc.
- Critical Technology Elements (CTEs).

For potential and designated ACAT I and ACAT IA programs, and for each Joint military or business requirement for which the Chairman of the JROC or the Investment Review Board is the validation authority, the Director of Cost Assessment and Program Evaluation (CAPE) develops and approves study guidance for the AoA.

The CAPE provides the AoA Study Guidance to the DoD Component or organization designated by the MDA or, for ACAT IA programs, to the office of the principal staff assistant responsible for the mission area, prior to the Materiel Development Decision and in sufficient time to permit preparation of the AoA Study Plan prior to the decision event. Per DoDI 5000.02 (Para 5(d)(1)(a) – page 13), programs coordinate the study plan with the MDA and gain approval from CAPE prior to the Materiel Development Decision. The designated DoD Component or other organization, or the principal staff assistant designates responsibility for completion of the study plan and the AoA.

At the Materiel Development Decision, the CAPE (or DoD Component equivalent) presents the AoA Study Guidance, and the AoA lead organization presents the AoA Study Plan. In addition, the Component provides the plan to staff and fund the actions preceding the next decision point (usually Milestone A) including, where appropriate, competitive concept definition studies by industry. If the Materiel Development Decision is approved, the MDA designates the lead DoD Component; determines the acquisition phase of entry; and identifies the initial review milestone, usually, but not always, a specific milestone as described in one of the program models.

In accordance with DoDI 5000.02 (Encl. 1, Table 2 – page 33), the PM provides the final AoA to CAPE not later than 60 calendar days prior to the Milestone A review (or the next decision point or milestone, as designated by the MDA). Not later than 15 business days prior to the Milestone A review, CAPE evaluates the AoA and provides a memorandum to the MDA, with copies to the head of the DoD

Component or other organization or principal staff assistant assessing whether the analysis was completed consistent with CAPE study guidance and the CAPE-approved study plan.

Within the memorandum, CAPE assesses:

- The extent to which the AoA:
  - Examines sufficient feasible alternatives.
  - Considers trade-offs among cost, schedule, sustainment, and required capabilities for each alternative considered.
  - Achieves the affordability goals established at Materiel Development Decision and with what risks.
  - Uses sound methodology.
  - Discusses key assumptions and variables, and sensitivity to changes in these.
  - Bases conclusions or recommendations, if any, on the results of the analysis.
  - Considers the fully burdened cost of energy (FBCE), where FBCE is a discriminator among alternatives.
- Whether additional analysis is required.
- How the AoA results are used to influence the direction of the program.

For more information on AoAs, see the DAG, CH 2.2.3.

CH 8–3.5.3 System Threat Assessment Report

Note*:* The Validated Online Life Cycle Threat (VOLT) is being developed to replace the STAR. Once approved, this section will be updated.

The System Threat Assessment Report (STAR) is the authoritative, system-specific threat capabilities document. The STAR describes the threat to be countered and the projected threat environment.

Based on DoDI 5000.02 (Encl. 4, para 5(c) – page 68), T&E personnel use the STAR as a reference for developing T&E plans, T&E resources and capability requirements, test scenarios, other T&E planning documents, as well as a guide for defining the threat environment for a mission-oriented context.

MDAP and MAIS programs require a unique, system-specific STAR, which is prepared by the appropriate Service Intelligence support, and the process is validated by the Defense Intelligence Agency (DIA). In accordance with DoDI 5000.02 (Encl 1, Table 2 – page 39), the assessment is required to be updated and validated at every acquisition milestone, although Services can update the document more frequently. All programs, unless waived by the MDA, must have a validated STAR in place at milestones beginning at Milestone A through Full Rate Production/Full Development (FRP/FD) at major decision points (and at program initiation for shipbuilding programs) unless waived by MDA. MDAP and MAIS programs require a unique, system-specific STAR. The assessment is system-specific to the degree that the system definition is available at the time the assessment is being prepared, and addresses projected adversary capabilities and maintains projections of technology and adversary capability trends over the next 20 years. DIA co-chairs the Threat Steering Group (TSG) for ACAT ID STARs with the producing command or center. STARs for ACAT IC MDAPs and System Threat Assessments (STAs) for ACAT II non-MDAPs are prepared and validated by the lead Service in accordance with Service regulations.

The T&E WIPT leverages the STAR (understand the threat) with other acquisition documents (e.g., CDD, SEP, PPP, etc.) when developing the T&E Strategy (Part III of the TEMP). The T&E WIPT refines the threat information found in the STAR to establish threat requirements for T&E. Since threats continue to evolve and mature with time, the T&E WIPT ensures the latest DIA, DoD Component intelligence agency, and/or Service intelligence organization validated threat assessments are considered for T&E-specific threat requirements and incorporated into all threat-related acquisition documentation.

The T&E WIPT ensures adequate threat resources, such as Modeling and Simulation, threat surrogates, and targets are documented in the TEMP resource section (Part IV, 4.2.8.), and adequate validation and accreditation processes are completed in time to support required testing.

Refer to the DAG, CH 7.4.1.4. for more information on the STAR.

CH 8–3.5.4 Acquisition Strategy

The Acquisition Strategy (AS) is the PM's plan for program execution across the entire program life cycle. It is a comprehensive, integrated plan identifying the acquisition approach, and describes the business, technical, and support strategies the PM plans to employ to manage program risks and meet program objectives. The strategy evolves over time and continuously reflects the current status and desired goals of the program.

The AS defines the relationship between the acquisition phases and work efforts, and key program events such as decision points, reviews, contract awards, incentive structure, test activities, production lot or delivery quantities, operational deployment objectives, and any planned international cooperation and exportability. The strategy must reflect the PM's understanding of the business environment; technical alternatives; small business strategy; costs, risks, and risk mitigation approach; opportunities in the domestic and international markets; and the plan to support successful delivery of the capability at an affordable life-cycle price, on a realistic schedule.

A central element of all acquisition strategies is an executable plan to use developmental and operational testing to assess design, development, performance, operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality. DoDI 5000.02 (Encl. 1, Table 2 – page 31) requires an approved AS at Milestone A. Once approved by the MDA, the AS provides a basis for more detailed planning.

The PM includes the Chief Developmental Tester and the T&E WIPT in the development of the AS so the strategy for T&E fully supports the program's approach. The AS includes a description of the test program for both the contractor and the government. It also includes a description of the test program for each major phase of a major system acquisition and a discussion of the extent of testing accomplished before LRIP.

Refer to the DAG, CH 1.4.1. for more information on acquisition strategies.

CH 8–3.5.5 Systems Engineering Plan

The Systems Engineering Plan (SEP) documents key technical risks, processes, resources, metrics (Technical Performance Measurement (TPMs) and other metrics), SE products, quality control, and completed or scheduled SE activities. The SEP is a living document updated as needed to reflect the program's evolving SE approach and/or plans and current status. The purpose of the SEP is to help PMs develop, communicate, and manage the overall systems engineering (SE) approach guiding all technical activities of the program.

T&E personnel use the SEP as a reference for developing their strategy for T&E, evaluation framework (Developmental Evaluation Framework (DEF) and Operational Evaluation Framework (OEF)), TEMPs, test plans, and other planning documents. In compliance with DoDI 5000.02 (Para 5(a)(4)(f) – page 3), PMs will prepare a SEP as a management tool to guide the SE activities on the program. The SEP Outline identifies the minimum expected content to be addressed in the SEP. The SEP should be consistent with and complementary to the Acquisition Program Baseline (APB), Acquisition Strategy (AS), Test and Evaluation Master Plan (TEMP), Program Protection Plan (PPP), Life Cycle Sustainment Plan (LCSP), and other program plans as appropriate. The SEP is written in a common language to clearly communicate what the program plans to do in each phase of the acquisition life cycle and is written to avoid redundancy and maintain consistency with other planning documents.

Test and evaluation personnel focus on the areas listed in Table 3, based on the SEP Outline.

Table 3: T & E Focus Areas in System Engineering Plan

Chapter	Relevant Content
2.1.	Architectures and Interface control: Look for architecture products that may support test planning such as physical and functional interfaces.
2.2.	Technical Certifications: Include test activities to obtain certifications in Table 2.2.-1
3.1.	Technical Schedule and Schedule Risk Assessment: Ensure test activities are included in the schedule (Figure 3.1.-1). Discuss with the systems engineer, potential schedule risks that may impact testing.
3.4.4.	Engineering Team Organization and Staffing: Check if T&E WIPT is correctly described.
3.6.	Technical Performance Measures and Metrics: TPMs enable program managers, systems engineers, and senior decision-makers to: (1) gain quantifiable insight to technical progress, trends, and risks; (2) empirically forecast the impact on program cost, schedule, and performance; and (3) provide measurable feedback of changes made to program planning or execution to mitigate potentially unfavorable outcomes. TPMs can be traced to KPPs/KSAs, Critical Technology Elements (CTE), or key technical risks, which should be verified and/or validated by test. Determine intermediate testing and data required to support this. The TEMP reliability growth curve should be consistent with the reliability growth curve in the SEP. Critical Technical Parameters described in the TEMP can be traced to the TPMs in the SEP.
4.4.	Technical reviews: Discuss test data that may be required to support engineering reviews such as the Critical Design Review (CDR), System Verification Review (SVR), and Functional Configuration Audit (FCA).
Table 4.6.-2	Reliability, Availability, and Maintainability (RAM) Activity Planning and Timing: Ensure RAM test events are included. Discuss with the system engineer how test supports Failure Reporting, Analysis and Corrective Action System (FRACAS) activities.
4.7.	Engineering Tools: Determine interfaces between the systems engineering requirements tools in the SEP and the common T&E database in the TEMP.

Refer to the DAG, CH 3.2.2. for more information on the SEP.

CH 8–3.5.6 Program Protection Plan

In accordance with DoDI 5000.02 (Encl. 1, Table 2 – page 37), T&E personnel use the Program Protection Plan (PPP) as a reference for developing test plans, test resource and capability requirements, and other planning documents; and identifying how T&E processes protect critical information about the program from being revealed to unauthorized personnel. Program Protection is the department's holistic approach for delivering trusted, secure systems and is used to ensure programs adequately protect their technology, components, and information throughout the acquisition process.

The PPP, written by the program office, officially documents the protection plan for a given acquisition program. The PPP protects the system from foreign collection, design vulnerabilities, supply chain exploitation, tampering, and battlefield loss. The program office takes an end-to-end system view when developing and executing the PPP (external, interdependent, or government furnished components that may be outside the PM's control must be considered). The PPP provides a usable reference within the program for understanding and managing the full spectrum of program and system security activities. Programs update the PPP as threats and vulnerabilities change or are better understood.

The Chief Developmental Tester, in coordination with the T&E WIPT, uses the PPP (and the appended Acquisition Cybersecurity Strategy) as an input when developing a program's T&E strategy and individual test plans. The PPP provides information on a program's critical missions, critical functions, critical components, threats, vulnerabilities, and threat countermeasures. This information can be used to guide and focus testing. Testing may reveal vulnerabilities that, when exploited, may have an impact on mission completion.

Refer to the DAG, CH 9.2.3. for more information on the Program Protection Plan.

CH 8–3.5.7 Cybersecurity Strategy

In accordance with DoDI 8500.01, Cybersecurity, (Encl. 3, para 2(c)(2) – page 29), a Cybersecurity Strategy (formerly known as the Information Assurance (IA) strategy) describes the program's planned cybersecurity risk management. All acquisition of qualifying information technology (IT) must have an adequate and appropriate cybersecurity strategy that will be reviewed prior to acquisition milestone decisions and acquisition contract awards in accordance with P.L. 106-398 SEC. 811 (reference e(3)(G)), and must plan for developmental test oversight by DASD(DT&E) and operational test oversight by DOT&E.

In accordance with DoDI 5000.02 (Encl. 11, para 6(b) – page 93), all acquisition of systems containing IT, including National Security Systems (NSS), will have a Cybersecurity Strategy. Beginning at Milestone A, the program manager will submit the Cybersecurity Strategy to the DoD Component Chief Information Officer (CIO) for review and approval prior to milestone decisions or contract awards. For ACAT ID and all ACAT IA, the DoD CIO reviews and approves the strategy; for all other IT and NSS programs, the DoD Component CIO reviews and approves the strategy.

The Chief Developmental Tester, in coordination with the T&E WIPT, will review the Cybersecurity Strategy and leverage it in the development of the TEMP. Test organizations review the cybersecurity strategy for test data and test events needed to support certification. The Chief Developmental Tester, in coordination with the Lead DT&E Organization, ensures test events (including Cooperative Vulnerability Identification and Adversarial Cybersecurity DT&E activities) are planned early during developmental testing to avoid late identification of cyber weaknesses during operational testing.

Refer to the DAG, Chapter 6.3.10.1. for more information on cybersecurity.

CH 8–3.5.8 Security Plan

In accordance with DoDI 8510.01 (Encl. 6, para 1(d) – page 27), Risk Management Framework (RMF) for DoD Information Technology (IT), the Security Plan provides an overview of the security requirements for the system, system boundary description, the system identification, common controls identification, security control selections, subsystems security documentation (as required), and external services security documentation (as required). The plan can also contain, as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.

The Information System Security Manger (ISSM) typically prepares the Security Plan. The Chief Developmental Tester, in coordination with the T&E WIPT, will review the Security Plan and leverage the

plan in the development of the TEMP. The Chief Developmental Tester invites the ISSM to participate in the T&E WIPT, thus allowing a cross pollination of knowledge in TEMP development.

CH 8–3.5.9 Security Assessment Plan

The Security Assessment Plan contains selected controls and their corresponding security control assessment with a detailed roadmap of how to conduct such an assessment.

In accordance with DoDI 8510.01 (Encl. 6, para 2(d)(1) – page 32), Security Assessment Plans apply to those systems required to follow the Risk Management Framework. This plan is reviewed and approved by the Component Authorization Official (CAO).

As this plan contains the systems roadmap for selected control assessment, it is recommended that the Chief Developmental Tester include the Security Control Assessor (SCA) as part of T&E WIPT during TEMP development. In this way, there can be a collaboration of efforts between the Security Assessment Plan and TEMP for better alignment and synergy of effort. Of note, the Security Assessment Plan does not include such areas as schedule (when selected controls are assessed) and required recourses (to assess the selected controls). The T&E WIPT references the program Security Assessment Plan with the TEMP and depicts the schedule of control assessment in Part II and required resources in Part IV. This allows the PM to visualize the holistic assessment effort.

CH 8–3.5.10 Acquisition Program Baseline

The Acquisition Program Baseline (APB) is the agreement between the MDA and the PM, and his or her acquisition chain of command, used for tracking and reporting the life of the program or program increment. T&E personnel use the APB as a reference for developing test plans and schedules, test resource and capability requirements, and other planning documents, in an effort to ensure the strategy for test and evaluation remains consistent with the program's goals and objectives. DoDI 5000.02 (Encl. 1, Table 2 – page 31) requires every PM to propose and document program goals prior to, and for approval at, program initiation for all ACAT programs. For Major Defense Acquisition Programs (MDAPs), the APB satisfies the requirements in 10 USC 2435 and 2220. DoDI 5000.02 (Encl. 1, Table 3 – page 40) mandates the use of an APB for all other ACAT programs.

A separate APB is required for each increment of an MDAP or MAIS program, and each sub-program of an MDAP. Increments can be used to plan concurrent or sequential efforts to deliver capability more quickly and in line with the technological maturity of each increment. When an MDAP requires the delivery of two or more categories of end items that differ significantly in form and function, subprograms may be established.

Program goals consist of an objective value and a threshold value for each Key Performance Parameter (KPP) and Key System Attribute (KSA) parameter. Cost, schedule, and performance are intrinsically linked, and the objective and threshold values of all program goals are developed with these relationships in mind. The PM has responsibility for managing the trade space between program objectives and thresholds within the bounds of cost, schedule, and performance. The APB includes affordability caps for unit production and sustainment costs. Affordability caps are established as fixed cost requirements equivalent to KPPs.

The PM derives the APB from the users' performance requirements, schedule planning and requirements, and best estimates of total program cost consistent with projected funding. The sponsor of a capability needs document (i.e., Capability Development Document (CDD) or Capability Production Document (CPD)) provides an objective and threshold for each attribute that describes an aspect of a system or capability to be developed or acquired. The PM uses this information to develop an optimal product within the available trade space. APB parameter values represent the program as it is expected to be developed, produced and/or deployed, sustained, and funded.

Refer to the DAG, CH 8.3.5.10. for more information on APBs.

CH 8–3.5.11 Cost Analysis Requirements Description

For Acquisition Category (ACAT) I and ACAT IA programs, the Cost Analysis Requirements Description (CARD) is used to formally describe the acquisition program for purposes of preparing both the DoD Component Cost Estimate and the Cost Assessment Independent Cost Estimate. DoDI 5000.02 (Encl. 1, Table 2 – page 34) specifies that MDAPs and MAIS provide a CARD in support of major milestone decision points (Milestone A and Milestone B, with updates at the Development Request for Proposal (RFP) Release Decision, Milestone C Decision, and FRP/FD Decision).

The Chief Developmental Tester ensures the test portion of the program definition is sufficiently defined for an adequate estimate. The tester also reviews the cost estimates resulting from the CARD to ensure reasonable funding and that the funding is included in the Resources section of the TEMP. Finally, cost estimates for testing eventually appear in the Research, Development, Test & Evaluation (RDT&E) Exhibits (specifically R-2 and R-3 for test), which go to the President and Congress, and the T&E Budget Submissions (T&E-1), which go to the DoD.

Refer to the DAG, CH 2.3.5. for more information on the CARD.

CH 8–3.5.12 Life-Cycle Sustainment Plan

The Life Cycle Sustainment Plan (LCSP) describes sustainment influences on system design and the technical, business, and management activities to develop, implement, and deliver a product support package that maintains affordable system operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality over the system life cycle, and seeks to reduce cost without sacrificing necessary levels of program support. In accordance with DoDI 5000.02 (Encl. 6, para 4(b) – page 81), during the Engineering and Manufacturing Development (EMD) phase it is critical to have robust testing to ensure reliability requirements are met. As the design matures, the trade space for sustainment solutions narrows and the sustainment strategy becomes more refined.

CH 8–3.5.13 Information Support Plan

The Information Support Plan (ISP) serves as a key document in achieving interoperability certification. The ISP describes Information Technology (IT) and information needs, dependencies, and interfaces for programs in all acquisition categories. It focuses on the efficient and effective exchange of information that, if not properly managed, could limit or restrict the operation of the program from delivering its defined capability. The Net-Ready Key Performance Parameter (NR-KPP) identified in the CDD or CPD will also be used in the ISP to identify support required from external information systems. Bandwidth requirements data will also be documented in the ISP.

A draft ISP is due at the Development RFP Release Decision. An approved ISP is required at Milestone B and Milestone C, in accordance with DoDI 5000.02 (Encl. 1, Table 2 – page 35). T&E personnel use the NR-KPP and the ISP to identify how the system (key interfaces, components, and dependencies) needs to be tested and evaluated for the following abilities: users can enter and manage on a network; users can effectively exchange information; and the system supports military operations. The ISP and a CONOPS/OMS/MP can be used to develop good test scenarios for evaluating key information/data exchanges that have an impact on mission success. The TEMP should include the testing of critical interfaces in as close to a mission environment (including a cyber-contested environment) as possible. Include DT&E Interoperability events (contractor and government) that focus on key information/data exchanges as part of the overall T&E program. When feasible, plan interoperability testing as part of other test events (such as cybersecurity testing, Risk Management Frame (RMF) security controls assessment activities, functional testing, etc.). Document the test resources for interoperability events (e.g. Facilities, People, Test Environment, Funding, etc.) in the TEMP. Specific criteria defined at Milestone B, and included in the Milestone B Acquisition Decision Memorandum (ADM), may require the system to demonstrate interoperability prior to Milestone C. Programs should plan to obtain an Interim Authorization To Test (IATT) prior to demonstrating interoperability, in accordance with DoDI 5000.02 (Encl. 13, para 4(c)(2) – page 101).

CH 8–3.5.14 Life Cycle Mission Data Plans

In accordance with DoDD 5250.01 (Para 4(c) – page 2) and DoDI 5000.02 (Encl. 1, Table 2 – page 36), Life Cycle Mission Data Plans (LMDPs) are required for Intelligence Mission Data (IMD)-dependent programs. Intelligence Mission Data are defined as DoD intelligence-derived information used for programming platform mission systems in development, testing, operations and sustainment, including, but not limited to, the following functional areas: intelligence signatures, electronic warfare integrated reprogramming (EWIR), order of battle (OOB), characteristics and performance (C&P), and geospatial intelligence (GEOINT).

The LMDP defines specific IMD requirements for a program, and becomes more detailed as the system progresses toward IOC. During development of T&E strategies and plans, IMD requirements are identified based on the need to verify and validate detection and identification functionality for DT&E, and for operational effectiveness and operational survivability for OT&E. The TEMP should define specific intelligence requirements to support program developmental and operational test and evaluation. The LMDP should include information on IMD data existing within the program (modeling and simulation or measured physical parameters) for sensor or algorithm development, or for testing purposes.

Refer to the DAG, CH 7.4.1.3., for more information on Life Cycle Mission Data Plans (LMDPs) and DAG, CH 7.4.2., Intelligence Mission Data (IMD).

CH 8–3.6 Test & Evaluation Master Plan

The Test and Evaluation Master Plan (TEMP) is a document that describes the overall structure and objectives of the T&E program and articulates the necessary resources to accomplish each phase, in accordance with DoDI 5000.02 (Para 5(a)(4)(f) – page 3). It provides a framework within which to generate detailed T&E plans and documents schedule and resource implications associated with the T&E program. The TEMP serves as the overarching document for managing a T&E program.

In accordance with DoDI 5000.02 (Encl. 4, para 2(c) – page 65) and DoDI 5000.02 (Encl. 5, para 1(b) – page 69), the TEMP identifies the necessary DT&E, OT&E, and LFT&E activities. It relates program schedule, test management strategy and structure, and required resources to: KPPs and KSAs, as identified within the Capability Development Document (CDD); Critical Operational Issues (COIs); and Critical Technical Parameters (CTPs) developed by the Chief Developmental Tester, in collaboration with the Chief Engineer/Lead System Engineer, and coordinated with the T&E WIPT.

The TEMP includes objectives and thresholds documented in the CDD, CPD, evaluation criteria, and milestone decision points. For multi-Service or Joint programs, a single integrated TEMP is required. Component-unique content requirements, particularly evaluation criteria associated with COIs, can be addressed in a Component-prepared annex to the basic TEMP.

In accordance with DoDI 5000.02 (Encl. 4, para 3(d) – page 65), the PM uses the TEMP as the primary planning and management tool for all test activities starting at Milestone A. The PM will prepare and update the TEMP at Milestone B and to support the Development RFP Release Decision and FRP/FD decision points. Additionally, the TEMP will have to be updated prior to Milestone C based on the CPD, and any remaining DT&E prior to IOT&E, and updates to IOT&E.

Program Management Offices (PMOs) develop a TEMP (and subsequent updates) to document the following:

- Roles and responsibilities, including Chief Developmental Tester and Lead DT&E Organization.
- Certification requirements necessary for the conduct of T&E.
- An event-driven T&E schedule.
- The T&E strategy aligned with and supporting the approved acquisition strategy to provide early identification of design and integration issues and adequate, risk-reducing T&E information to support decisions.

- The integration of developmental and operational tests into an efficient test continuum.
- The strategy for T&E.
- Starting at Milestone A, a developmental evaluation methodology.
- Starting at Milestone B, a developmental evaluation framework.
- The T&E resources, which should be in alignment with the CARD and T&E budget exhibits (ACAT I programs).
- The test and evaluation strategies to efficiently identify technology and functionality limitations and capabilities of alternative concepts to support early cost performance trade-off decisions.
- Adequate measures to support the program's reliability growth plan and requirements for a Reliability, Availability, Maintainability Cost (RAM-C) Rationale Report defined in DoD RAM Cost Rationale Manual, for Milestones B and C.
- The modeling and simulation approach and where it is used in the test events, including the resources required and methodology for their verification, validation, and accreditation (VV&A); and how the PM and OTA plan to accredit M&S for OT use.
- A T&E approach that stresses the system under test to at least the limits of the Operational Mode Summary/Mission Profile, and for some systems, beyond the normal operating limits to ensure the robustness of the design.
- The plan for demonstration of maturity of the production process through production qualification testing (PQT) of low-rate initial production (LRIP) assets prior to full-rate production (FRP).
- The plan for using the System Threat Assessment (STA) or System Threat Assessment Report (STAR) as a basis for scoping a realistic test environment.
- The approach for demonstrating performance against threats and their countermeasures as identified in the Defense Intelligence Agency (DIA), DoD Component intelligence agency, or Service intelligence organization validated threat document.
- The cybersecurity test and evaluation approach. Additionally, the approach should coordinate development of the Security Assessment Plan with the development of the TEMP in support of the Risk Management Framework (RMF) process. (The RMF process and certification can be a useful entrance criterion for cybersecurity T&E, but it does not obviate the need for T&E.)
- The plan for Joint interoperability assessments required to certify system-of-systems interoperability.
- For business systems, the identification of the certification requirements needed to support the compliance factors established by the Office of the Under Secretary of Defense (Comptroller) (USD(C)) for financial management, enterprise resource planning, and mixed financial management systems.
- A system-of-systems network architecture diagram, including removable media and laptops, etc., for cybersecurity assessment.

The following contains a basic TEMP outline, which highlights the key TEMP topics needing addressed. Go to T&E Policy & Guidance for an editable TEMP Format and additional TEMP information.

Refer to the TEMP Guidebook for more detail regarding TEMP content.

TEMP FORMAT	
PART I – Introduction	
1.1.	Purpose
1.2.	Mission Description
1.2.1.	Mission Overview
1.2.2.	Concept of Operations
1.2.3.	Operational Users
1.3.	System Description

4.2.6.	Test Targets and Expendables
4.2.7.	Operational Force Test Support
4.2.8.	Models, Simulations, and Test Beds
4.2.9.	Joint Operational Test Environment
4.2.10.	Special Requirements
4.3.	Federal, State, and Local Requirements
4.4.	Manpower / Personnel and Training
4.5.	Test Funding Summary
APPENDICES	
Appendix A	Bibliography
Appendix B	Acronyms
Appendix C	Points of Contact
The following appendices provide a location for additional information, as necessary	
Appendix D	Scientific Test and Analysis Techniques
Appendix E	Cybersecurity
Appendix F	Reliability Growth Plan
Appendix G	Requirements Rationale
Additional Appendices, as needed	

CH 8–3.6.1 T&E Resources

The PM, in coordination with the T&E WIPT, must identify and plan for all T&E resources (including Cybersecurity) needed to adequately support DT&E, OT&E, and LFT&E, in accordance with DoDI 5000.02 (Encl. 4, para 2(d) – page 65).

"Test and Evaluation Resources" refers to the elements necessary to plan, execute, and evaluate a test event or test campaign. These elements include funding, manpower for test conduct and support (e.g., cybersecurity teams, subject matter experts, additional testers, data collectors, trusted agents, etc.), test articles (e.g. system under test, accompanying assets, targets, threats, and expendables), models, simulations, test facilities, special instrumentation, frequency management and control, and base or facility support services. Programs identify one-of-a-kind T&E resources and long-lead items early in the acquisition process in order to allot adequate funding for development and use. In accordance with DoDI 5000.02 (Encl. 4, para 5(b) – page 68), programs must use existing DoD government T&E infrastructure unless an exception can be justified as cost-effective to the government.

In accordance with DoDI 5000.02 (Encl. 5, para 10 – page 74), all TEMPs will specify the T&E resources necessary to execute the T&E program, the organization responsible for providing each element, and when the elements are needed. Additionally, T&E funds are also stated in budgeting documents, such as the program's budget and T&E-1 exhibits.

T&E resources provided by the contractor must be identified in either the development or production contract.

CH 8–3.6.2 Requirements Rationale

In accordance with DoDI 5000.02 (Encl. 5, para 5(d)(2) – page 71), the TEMP provides a working link to the Component's operational rationale for the requirements in the Capability Development Document (CDD) or equivalent requirements document. If the rationale documented in the requirements document

is adequate to support test planning and evaluation, then no further clarification is necessary. DoDI 5000.02 (Encl. 4, para 4(a) – page 66) states that DT&E activities will start when requirements are being developed to ensure that key technical requirements are measurable, testable, and achievable. In cases where the requirement is derived or transformed for testability or the operational rationale is unclear, this annex explains the operational rationale and/or the derivation of the metric as well as the chosen numerical thresholds. For example, requirements documents often specify the reliability requirement in terms of the probability of completing a reference mission; for testability, this is often translated to a mean time between failures. In this case, the assumptions supporting the derivation of the mean time between failures should be documented in the requirements rationale annex as well as the original justification for the probability of mission completion.

CH 8–3.6.3 Critical Technical Parameters

Acquisition programs have hundreds or thousands of technical parameters that need to be addressed during development.

CTPs are used in developmental test and evaluation to identify critical system characteristics that, when measured and achieved, allow the attainment of a desired user capability, In accordance with DoDI 5000.02 (Encl. 4, para 4(b)(1) – page 66). CTPs are measures derived from desired user capabilities and are focused on critical design features or risk areas (e.g., technical maturity, Critical Technology Elements (CTEs), physical characteristics, technical measures, or reliability, availability, and maintainability (RAM) issues). If CTPs are not achieved during development, they will indicate a significant risk in the delivery of required user capabilities. CTPs link to high risk areas having an impact on program success. CTPs are tracked during EMD and may need to evolve/change as the system matures. It may also be necessary to resolve existing CTPs and identify new CTPs as the system progresses during development. The status of achieving CTPs is provided to the Milestone Decision Authority as part of the DT&E Program Assessment at Milestone C or Limited Deployment. Any CTP not resolved prior to entering the LRIP decision should be documented and action plans provided that resolve the unresolved CTPs prior to the FRP Decision Review.

Technical Performance Measures (TPMs) are metrics and measures evaluating technical progress (i.e., product maturity) as part of the systems engineering process. Some TPMs can be CTPs; however, every TPM is not a CTP. TPMs are measured through inspection, demonstration, test, and analysis. Systems Engineering (SE) uses TPMs to balance cost, schedule, and performance throughout the life cycle when integrated with other management methods such as the Work Breakdown Structure (WBS) and Earned Value Management System (EVMS). Examples of TPMs include measures such as weight, speed, volume, cross-section, power, cooling, bandwidth, throughput, lines of code, reliability, maintainability, etc.

CTPs measure the critical system characteristics that, when achieved, enable the attainment of desired operational performance capabilities (in the mission context). CTPs do not simply restate the KPPs and/or KSAs. Each CTP has a direct or significant indirect correlation to a KPP and/or KSA that measures a physical characteristic essential to the evaluation of the KPP or KSA, In accordance with DoDI 5000.02 (Encl. 5, para 5(e)(2)(c) – page 71). CTPs are directly measurable during developmental testing and included as part of the developmental evaluation plans included in the TEMP. Examples of CTPs include fuel consumption, engine thrust, data upload time, latency, bore sight accuracy, etc.

The Chief Developmental Tester has responsibility for collaborating with the program's Chief or Lead Systems Engineer on the identification of CTPs. The Lead DT&E Organization can assist in the development of CTPs as well as the developmental evaluation plans for the CTPs. The evaluation of CTPs is important in assessing the maturity of the system and to inform the PM as to whether the system is on (or behind) the planned development schedule or is likely (or not likely) to achieve an operational capability, but is not the only component of projecting mission capability. The projection of mission capability requires an evaluation of other areas such as interoperability of systems and subsystems in the mission context, when used by a typical operator. CTPs associated with the systems/subsystems can provide a basis for selecting entry or exit criteria that needs to be demonstrated to make a decision to

continue with the next major developmental test or test phase. CTPs are a driver in the scope/magnitude of the T&E program.

CH 8–3.6.4 T&E Plans

This section provides information on detailed test and evaluation planning for test or data collection events or test series identified in the TEMP, in accordance with DoDI 5000.02 (Encl. 4, para 6(a) – page 68) and DoDI 5000.02 (Encl. 5, para 1(b) – page 69).

CH 8–3.6.4.1 Evaluation Plans

Planning for a specific test or data collection event or test series is preceded by an evaluation plan. Evaluation plans are to be directly traceable to the evaluation framework for the program, include expected results, and are informed by WIPTs to ensure the meeting of all data needs, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(2)(d) – page 67).

CH 8–3.6.4.2 Test or Data Collection Plans

Test or data collection plans come in a variety of formats and styles but contain the following content:

- Objectives.
- Test schedule.
- Test resource (facilities, instrumentation requirements, personnel, test articles, test support equipment, etc.).
- Data collection plan.
- Test techniques.
- Test points.
- Evaluation criteria.
- Limitations.
- Test management structure and information.
- Safety considerations.

In accordance with DoDI 5000.02 (Encl. 4, para 3(d) – page 65), test plans document why tests are accomplished and what the goal(s) of the test are (the objectives), how tests are conducted (the test techniques, test points, and execution plan), what conditions and factors are controlled and varied in the test, what data are acquired (including the instrumentation requirements), how data are used to answer the objectives (the data analysis plan), and when and what types of reports are needed (management information). Test plans are the vehicles that translate test concepts and statistical/analytical test design into concrete resources, procedures, actions, and responsibilities. The size and complexity of a test program and its associated test plan are determined by the nature of the system being tested and the type of testing that is accomplished. Some major weapon systems may require large numbers of separate tests to satisfy test objectives, and thus require a multi-volume test plan; other testing may be well-defined by a relatively brief test plan. Modeling and simulation may be used for the realization of proposed test scenarios (including test plans), instrumentation set-up, distribution and adequacy of resources, and schedules. Schedules allow for system-under-test set-up, instrumentation calibrations, weather conditions, availability of test support personnel, and other support.

Government Developmental Test Plans. The government test plan provides explicit instructions for the conduct of tests and sub-tests. It governs test control, test configurations, data collection, data analysis, and administrative aspects of the tester's operations. The Lead DT&E Organization and or test officer prepares a test plan in accordance with the directions provided by the Chief Developmental Tester, TEMP, and test directive, and determines the best plan for the testing of the system for the area(s) assigned.

Contractor Developmental Test Plans. If the data from the contractor DT&E are to be used by the Chief Developmental Tester, the test plan should reflect all the requirements to support the systems evaluation. When the system contractor is conducting DT&E, whether at the contractor's facilities or government test site, a test plan is provided to the Chief Developmental Tester for review and approval, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(2)(d) – page 67).

Operational Test Plans. The Operational Test Agency (OTA) plans, develops, and executes the Operational Test Plan (OTP), in accordance with DoDI 5000.02 (Encl. 5, para 11(a)(3) – page 75). An OTP is prepared for an operational assessment (OA), an Initial Operational Test and Evaluation (IOT&E), a Follow-on Operational Test and Evaluation (FOT&E), and other operational test events identified in the TEMP. The OTP documents adequate testing to assess whether the system under test is operationally effective and operationally suitable when used by representative, properly trained personnel in an operationally realistic environment. In the case of OA, the OTP documents testing that supports progress towards the assessment of operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality. The OTP documents the test design, supporting methodology, and analytic details required for the specific operational test. Additionally, the cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Assessment (AA) test plans must be approved by DOT&E in order to get the credit for these tests.

CH 8–3.7 Key Considerations in T&E Strategy Development

The following are key considerations in developing the TEMP, in accordance with DoDI 5000.02 (Encl. 4, para 2(c) – page 65).

CH 8–3.7.1 Use of Government Test Facilities for T&E

In accordance with DoDI 5000.02 (Encl. 4, para 5(b) – page 68), programs will use DoD government T&E capabilities and invest in government T&E infrastructure unless a program can justify the exception as cost-effective to the government. In addition, PMs will conduct a Cost Benefit Analysis (CBA) for exceptions to this policy and obtain approval through the TEMP approval process before acquiring or using non-government, program-unique test facilities or resources.

In accordance with DoDI 5000.02 (Encl. 4, para 3(f) – page 66), the PM must take full advantage of DoD ranges, laboratories, and other resources and programs; and consult with their Lead DT&E Organization to determine availability and adequacy of DoD or other government-owned test capabilities and resources to execute proposed T&E strategies. Approaches to resolving test capability and resource gaps are to be identified in the strategy for T&E.

The Test Resource Management Center (TRMC) can provide assistance in identifying available government test facilities. T&E WIPTs utilize their DASD(DT&E) representative to engage TRMC supporting staff experts on test ranges and facilities.

CH 8–3.7.2 Evaluation Methodology & Framework

This section describes both the developmental and operational evaluation approaches. Each approach consists of an evaluation methodology and an evaluation framework.

Part 3 of the TEMP Format includes the program's evaluation implementation plans. Parts 3.2 and 3.3 include the developmental evaluation methodology and framework, and parts 3.5 and 3.6 include the operational evaluation methodology and framework. In accordance with DoDI 5000.02 (Encl. 4, para 5(a)(10) – page 68), programs update both evaluation approaches with each TEMP update to account for system maturity, changes to source documents (e.g. CDD/CPD, AS, STAR, SEP, ISP, etc.), or contractor down select.

CH 8–3.7.2.1 Developmental Evaluation Methodology

As the system design matures, data or evaluations are needed to inform the program manager and other decision-makers on the progress the system is making towards meeting system requirements and achieving desired performance. To ensure information is available to inform decisions in a timely manner, evaluation planning must precede test planning. The Developmental Evaluation Methodology identifies the essential information needed to inform major programmatic decisions.

In accordance with DoDI 5000.02 (Encl. 4, para 5(a)(11) – page 68), starting at Milestone A the TEMP will include a developmental evaluation methodology providing essential information on programmatic and technical risks as well as information for major programmatic decisions. Starting at Milestone B, the developmental evaluation methodology will become the Developmental Evaluation Framework (DEF), identifying key data that will contribute to assessing progress toward achieving system requirements. However, from the onset of the program's evaluation planning, it is recommended that programs use a DEF to logically organize the DT&E strategy.

To ensure T&E focuses on informing the program's decision-making process throughout the acquisition life cycle, Part 3.1 of the TEMP includes the key program decision points and the information needed to support them (see "Decision Support Key" example). Answers to the Decision Support Questions (DSQ) from the DEF and the Critical Operational Issues (COIs) from the Operational Evaluation Framework (OEF) provide the T&E information used to inform decisions throughout the program acquisition.

Once evaluation planning is complete, the DEF and OEF identify opportunities for integrated testing where shared test events can provide data for both the developmental and operational evaluations. A conscious effort is required by the DT&E and OT&E communities to leverage opportunities suited for integrated testing, whenever feasible.

A separate summary of decision points and the information needed to support them is included in a table (see "Decision Support Key" example) to serve as a quick reference for evaluations in Part 3.1 of the TEMP Format.

CH 8–3.7.2.2 Developmental Evaluation Framework

In accordance with DoDI 5000.02 (Encl. 4, para 5(a)(11) – page 68), starting at Milestone B, the DEF identifies key data contributing to assessment progress towards achieving: key performance parameters (KPPs), key system attributes (KSAs), critical technical parameters (CTPs), interoperability requirements, cybersecurity requirements, reliability growth, maintainability attributes, developmental test objectives, and others, as needed. In addition, it shows the correlation/mapping between test events, key resources, and the decision(s) supported.

The DEF guides development of the DT&E strategy by focusing the thought process on logically identifying the critical program decisions and defining the information needed to inform them, and finally the test and modeling and simulation (M&S) events needed to generate the data for the evaluation. Once complete, the DEF format, identified in TEMP Section 3.2, articulates the results.

The DT&E strategy is built by defining its components (decisions, Decision Support Questions (DSQ), capabilities, technical measures, and test/modeling and simulation events) and articulating them in the DEF. The components of the DT&E strategy and the DEF are:

- Decisions: Decision points throughout the acquisition life cycle, made by decision-makers ranging from the program manager (PM) to the Milestone Decision Authority (MDA), to be informed by DT&E-gained knowledge.
    - Decisions are listed in the first row of the DEF, forming the matrix's columns.
    - Decisions reflected in the DEF should represent major turning/decision points in the acquisition strategy needing DT&E information in order to make an informed decision.

Examples may include milestone decisions, key integration points, technical readiness decisions, etc.

- Decision Support Questions (DSQ): Questions capturing the essence of the information needed to make informed decisions.
  - Each DSQ to be used to inform a decision is listed in the second row of the DEF, forming sub-columns under each decision. For example, the answers to DSQ#1 through DSQ#3 will be used to inform Decision #1.
  - The DSQ phrases the question the decision-maker needs to have answered based upon the system evaluation during DT&E, to make an informed decision. For example, the decision to move forward with system integration may be informed with DSQ such as: (1) Are the components to be integrated performing as required? (2) Are the basic platform capabilities performing as required?
- Developmental Evaluation Objectives (DEO): The system's performance, interoperability, cybersecurity, and reliability capabilities to be evaluated.
  - The system's technical capabilities, or DEO, are those areas that must be evaluated to answer the DSQ to inform the program's decisions.
  - The DEO, divided into the functional areas of performance, interoperability, cybersecurity, and reliability, are listed in the first column of the DEF, forming the category rows of the matrix.
  - The DEO are derived from the major categories of technical capabilities listed in the system's Technical Requirements Document or top-level System Specification. For example, an aircraft's technical performance capabilities may include flight performance and mission communication.
- Technical Measures (TM): The top-level measures, or capability sub-categories that quantify the capabilities.
  - The TM and their reference within the technical requirements document are listed in the second and third columns of the DEF, adjacent to the capability they quantify, forming the individual rows of the matrix.
  - The TM or capability sub-categories are the means for quantifying system performance at a strategic level of detail. Each capability should have a few TM listed to capture, at a strategic level of detail (or "inch-deep/mile-wide"), how the capability will be quantified during the system's evaluation. The TM should not be all the requirements listed in the technical requirements document, nor should the DEF replicate the program's Verification Cross Reference Matrix (VCRM). For example, the aircraft's flight performance could be quantified by measuring Range/Payload, Take-off/Landing, Airfield Ops, Instrument Approach, and Emergency Ops.
- Data Sources: The test, modeling and simulation, or other events generating the data needed for system evaluation.
  - Where a DSQ needs information about a system capability in order to inform the decision point, the DEF identifies the data source for the evaluation.
  - The test, modeling and simulation events, or other data sources used for the evaluation of the TM/system capabilities are listed at the DEF cells at the intersection between the DSQ needing information and the capability/TM. For example, Decision #1 is informed by answering DSQ#1 through DSQ#3. DSQ#1 is answered by evaluating system performance capability #1 by measuring TM#1 through TM#3 using data gathered during DT#1 and M&S#1.

Upon program office request, DASD(DT&E) will deploy a DEF Core Team to assist the program in tailoring the DEF concept to the specifics of the program's information needs, by facilitating the discussion and building a draft DEF product for the program's TEMP.

Table 4: Development Evaluation Framework Essential Information

Functional Evaluation Area	Categorical groupings of functional areas brought forward or derived from baseline documentation (Performance, Reliability, Cybersecurity, or Interoperability).
Decision supported	The significant program decision points where data and information gathered during testing are used to make decisions or give program direction. Not limited to major acquisition milestones.
Decision Support Question	Key question related to Performance, Reliability, Cybersecurity, or Interoperability that, when answered, determines the outcome of an evaluation for the decision supported.
Key system requirements (KPPs, KSAs, CTPs, etc.) and T&E measures	One or more fields of requirements identification and performance measurement: • **Technical requirements document reference**. Provides references to sources of technical requirements about which information is sought for a decision supported. Performance or Detailed Specifications are the preferred sources. JCIDS documents may be used prior to the development of government specifications. • **Description** (of technical requirements). Short plain text description of the requirement or technical measurement. • **Technical measures**. CTP, applicable TPMs, metrics, benchmarks. These have units and values. May include intermediate levels of performance associated with decision supported.
Method (technique, process, or verification method)	Method/methodology by which the data and information are gathered. Could be a test, model, simulation, observation, inspection, etc.
Test Event	Name of the test event(s) or other verification event(s) providing data for the technical measures and information to answer the decision support question.
Resources	Brief reference may appear here. Detailed in TEMP Part IV.
Cross Reference	Used to refer to related requirements, capabilities, and line items to aid in requirements traceability, precedence, interdependency, and causality.

The TEMP Guidebook provides Developmental Evaluation Framework examples.

CH 8–3.7.2.3 Operational Evaluation Framework

In accordance with DoDI 5000.02 (Encl. 5, para 6(d) – page 72), the Operational Evaluation Framework summarizes the mission-focused evaluation methodology and supporting test strategy, including the essential mission and system capabilities that contribute to operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality. The framework identifies the goal of the test within a mission context, mission-oriented response variables, factors that affect those variables, and test designs for strategically varying the factors across the operational envelope, test period, and test resources. The Operational Evaluation Framework may also include standard measures of program progress including: Critical Operational Issue Criteria (COIC), KPPs, KSAs, CTPs, interoperability requirements, cybersecurity requirements, reliability growth, maintainability attributes, and others as needed. The Operational Evaluation Framework focuses on:

- The subset of mission-oriented measures critical for assessing operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality.
- Resource, schedule, and cost drivers of the test program.

The Operational Evaluation Framework shows how the major test events and test phases link together to form a systematic, rigorous, and structured approach to quantitatively evaluate system capability across the operational envelope. When structured this way, the framework also becomes a tool for synthesizing and justifying the resources necessary for an adequate test.

Table 5 below identifies information for inclusion in the Operational Evaluation Framework.

Table 5: Operational Evaluation Framework Essential Information

Goal of the Test	Typically, the goal is to characterize operational missions and/or capabilities across the operational envelope. • Describe the operational missions and/or capabilities assessed. • Link each mission/capability to at least one mission-oriented response variable. • Address the associated COI(s) or COIC, where applicable.
Mission-oriented Response Variables (T&E Measures)	Quantitative T&E measures provide criteria for mission accomplishment (not technical performance for a single subsystem) and comprehensively cover the reasons for procuring the system (the need).
	Also include the resource, schedule, and cost drivers of the test program.
Test Design	Factors affecting the mission-oriented response variables during operational employment of the system.
	Scientific and statistical method for strategically varying the factors across the operational envelope.
	Statistical measures of merit (power and confidence), where appropriate. • Provide power calculations for determining the effect of factors on the response variables.

	• When an experimental design includes multiple statistical measures of merit (e.g., separate power values for several factors (and their interactions).
	Effect sizes for observing identified factors and their interactions, where appropriate.
	Provide a brief justification and description of the test, when not utilizing a scientific approach to test planning.
	Only provide a summary in the Operational Evaluation Framework; the body of the TEMP includes detailed test design information or a STAT appendix and is referenced in the Operational Evaluation Framework.
Test Period	Include all operational test periods when collecting data (e.g., LUT, OA, IOT&E, FOT&E, etc.).
Resources	High-level summary of the resources (time, people, places, and things) needed to execute an adequate test.

The Operational Evaluation Framework also aids Integrated Testing by identifying opportunities for using DT data for OT evaluation. In cases where OT evaluation leverages DT, the Operational Evaluation Framework links to the supporting Developmental Evaluation Framework and summarizes procedures for ensuring data collected in DT are both appropriate and adequate for OT evaluation.

The Operational Evaluation Framework matures as the system matures. Insert the Operational Evaluation Framework in Section 3 of the TEMP if short (less than 2 pages), embedded as an Excel table/database, or provided as an annex. Each program remains unique and requires thoughtful trade-offs in applying this guidance. Programs can also use equivalent Service-specific formats identifying the same relationships and information.

CH 8–3.7.3 Reliability T&E

Initial reliability DT&E supports contractor design for reliability and assessment of design margins intended to provide system, subsystem, and component robustness, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(2)(e) – page 67) and DoDI 5000.02 (Encl. 5, para 6(c) – page 72). Even so, initial prototypes of complex systems will almost always have inherent reliability and performance deficiencies that generally could not have been foreseen and eliminated in the early design stages. To uncover and eliminate these deficiencies, T&E activities start early with prototypes and continue as the system hardware and software mature. Developmental tests are specifically planned and conducted to stress the system components to predetermined realistic levels at which inadequate design features will surface as system failures. These failures are analyzed, design modifications incorporated, and then the modified system is tested to verify the validity of the design change. This testing philosophy utilizes the test-analyze-fix-test (TAFT) procedure as the basic catalyst in achieving system reliability growth.

The ultimate goal of a reliability growth program is to increase system reliability to a stated requirement level by eliminating a sufficient number of inherent system failure modes. A successful system reliability growth program is dependent on several factors. First, an accurate determination must be made of the current system reliability status. Second, a test program must be planned that subjects the system to stress conditions that are adequate to uncover inherent failure models and to verify design modifications. Third, the Chief Developmental Tester must plan and resource the T&E activities required to support the "TAFT" procedure as part of the TEMP. To adequately control these as well as other factors inherent in the reliability growth process, it is important to track reliability growth throughout the testing program. This

is accomplished by periodically assessing system reliability at specified points in time during the development and comparing the current reliability to the planned level of achievement for that point in time. These assessments provide the necessary data and visibility to support the necessary corrective action activities.

Reliability assessment testing estimates the reliability of a component, subsystem, or production-representative system within operationally relevant conditions. The resulting reliability estimate can be compared to the reliability requirement and assessed in the context of the operational mission. Operational test organizations examine the implications of the achieved reliability in the context of the operational mission, which may lead to different conclusions than a simple comparison to the reliability requirement.

CH 8–3.7.3.1 Reliability Growth Testing

Reliability growth is achieved by eliminating initial design or manufacturing weaknesses in a system via failure mode discovery, analysis, and effective correction. Systems with comprehensive reliability growth programs are more likely to meet their development goals than systems without such programs. Activities of a comprehensive reliability growth program include:

- Initiating the reliability growth program from the beginning, as part of system design.
- Having a clear understanding of the intended mission(s) for the system, including the stresses associated with each mission, mission durations, and configuration control.
- Developing adequate requirements that are quantitative, mission-oriented, testable, achievable, reflect the desired reliability of the system, and cover the system's operational mission envelope.
- Establishing a reliability goal that supports being able to demonstrate the reliability requirement during developmental testing (DT) and operational testing (OT) with acceptable risk.
- Ensuring that the contract, and contracting and funding decisions support reliability growth efforts.
- Developing a reliability growth curve based on realistic assumptions that can be used as a tool to track progress during testing.
- Establishing intermediate reliability goals or entrance criteria and meeting these goals before proceeding to OT.
- Conducting testing that is of sufficient length and is representative of the system's operational mission profile.
- Supporting growth testing with reliability analyses that include Failure Modes and Effects Criticality Analysis (FMECA), Level of Repair analysis, reliability predictions.
- Establishing a Failure Reporting, Analysis, and Corrective Action System (FRACAS), Failure Review Board, and a RAM working group.
- Ensuring that reliability expectations during each phase of development are supported by realistic assumptions that are linked with systems engineering activities.
- Programs developing a path forward to address shortfalls when sufficient evidence exists that the demonstrated reliability is significantly below the growth curve.
- Ensuring the program is adequately resourced for engineering support to conduct failure analysis and corrective action solutions.

An effective Reliability Growth Program includes elements of planning, tracking, and projection that are part of an overall Reliability Growth Management strategy. MIL-HDBK-189C, Reliability Growth Management, provides more detail on all elements of reliability growth management. The goal of reliability growth planning is to optimize testing resources, quantify potential risks, and plan for successful achievement of reliability objectives. A well-thought-out reliability growth plan can serve as a significant management tool in identifying resources required to enhance system reliability and improve the likelihood of demonstrating the system reliability requirement.

In accordance with DoDI 5000.02 (Encl. 4, para 5(a)(2)(f) – page 67) and DoDI 5000.02 (Encl. 5, para 6(c)(2)(a) – page 72), as part of reliability growth planning, programs construct reliability growth planning curves (RGPC) to illustrate how reliability increases over time. The RGPC is a target; the curve does not

imply that inherent system reliability automatically grows to achieve these values. On the contrary, attainment of these values is feasible only with the incorporation of an adequate number of effective designs and/or process fixes. RGPCs for hardware and hybrid (hardware and software) systems are typically based on the U.S. Army Materiel Systems Analysis Activity (AMSAA) Planning Model based on Projection Methodology (PM2) or the Crow-Extended Planning Model. MIL-HDBK-189C provides more detail on RGPCs.

The reliability growth tracking curve (RGTC) provides a gauge to track the progress of the reliability efforts. This is done by determining whether system reliability is increasing with time (i.e., growth is occurring) and to what degree (i.e., growth rate), and estimating the demonstrated reliability during testing. Both the Duane Model and the AMSAA Reliability Growth Tracking Model (RGTM) may be used to model growth. MIL-HDBK-189C, Reliability Growth Management, provides more detail on RGTCs.

Reliability projection is an assessment of the reliability that can be anticipated at some future point in the development program given corrective action. Projection is based on the reliability achievement to date and engineering assessments of future program characteristics. It is a particularly valuable analysis tool when a program is experiencing difficulties, because it enables investigation of program alternatives.

Guidance for documentation of reliability growth in TEMPs is discussed in the TEMP Guidebook.

Reliability is measured, monitored, and reported throughout the acquisition process. Reliability measurements and estimates are recorded on the RGTC and compared to the RGPC. Reliability growth strategies for systems not meeting entrance and exit criteria are revised, at a minimum, at each Milestone to reflect current system reliability. When necessary, reliability growth continues after the full-rate production (FRP) decision.

Refer to the DAG, CH 3.4.3.19., Reliability and Maintainability Engineering, for more information on Reliability.

CH 8–3.7.3.2 Reliability Assessment Testing

Reliability assessments primarily estimate the reliability of a production-representative system under operationally realistic conditions, In accordance with DoDI 5000.02 (Encl. 4, para 5(a)(2)(e) – page 67). Test personnel conduct reliability assessments on systems with fixed-design configurations. Operational testing is commonly used to reach statistically valid decisions regarding whether an item has achieved its specified reliability under the realistic conditions in which the user is expected to operate the system. Operational test organizations examine the implications of the achieved reliability in the context of the operational mission, which may lead to different conclusions than a simple comparison to the reliability requirement. Therefore, testing is long enough to demonstrate both the reliability requirement and an operationally meaningful reliability. If the program successfully executes a Reliability Growth Program through DT and prior to the OT, the chance of demonstrating the required reliability during OT is high.

The most common test methodology for a reliability assessment is a fixed duration test; other methods include two-stage and sequential test plans. A fixed duration test provides the exact test duration during the test planning process, whereas other methods have variable test lengths, depending on the observed failures in testing. The length of a fixed duration test is determined by balancing the expected system reliability, test duration, and the statistical risks (producer’s risk versus consumer’s risk). Operating characteristic (OC) curves are used to determine either the minimally acceptable reliability or the test duration as a function of the statistical risks. The risks are related to the reliability growth goal. DOT&E does not require any specific values for producer’s and consumer’s risk in OT. The rationale for the selection of test risks derives from the specifics of each program.

OC curves are constructed assuming any statistical distribution. It is common for time- or distance-based reliability requirements to assume a constant failure rate (exponential distribution). For equipment that operates only once (a one-shot device) or cyclically (such as pyrotechnic devices, missiles, fire warning systems, and switchgear), testing based on operating time is inappropriate. For these pass/fail systems, the binomial distribution is used to construct the OC curve.

Refer to the TEMP Guidebook for more information on using operating characteristic curves to determine the length of a demonstration test.

CH 8–3.7.3.3 Reliability T&E Tracking

The reliability process weaves reliability engineering across the design, testing, tracking, and assessment activities during total development cycle of an acquisition program. The purpose of reliability T&E tracking is to assess the reliability improvement of a system during development. Reliability growth tracking provides decision-makers the opportunity to gauge the progress of the reliability effort for a system. The choice of a reliability tracking model is dependent on the management strategy for incorporating corrective actions in the system. The management strategy for some programs may require a corrective action for specific failures while other management strategies may not.

CH 8–3.7.3.4 Reliability T&E Tools

The purpose of reliability engineering is to influence system design in order to increase mission capability, decrease logistics burden, and decrease life-cycle cost of the product. Reliability engineering includes a set of design and test activities that start early during the Materiel Solution Analysis phase and continue through the Operations and Support phase. A comprehensive T&E program includes the use of reliability T&E tools to discover and mitigate failure modes throughout the development and production process. Accelerated test methods such as HALT and HASS are well-recognized industry reliability test and screening methods.

Highly Accelerated Life Testing (HALT)/Highly Accelerated Stress Screening (HASS). The most common application of accelerated testing such as HALT and HASS occurs with electronic equipment. HALT is used during development to determine the operating and destruct limits. HASS is used during production to screen components to detect latent flaws. Although general guidelines exist for implementing HALT and HASS, tailoring is needed on each item and application. HALT and HASS are focused on detecting and eliminating failure modes at the component and sub-component level so that corrective actions can be implemented before the start of system-level testing.

A comprehensive T&E program includes practices such as HALT and HASS to discover and mitigate failure modes throughout the development and production process. Although general guidelines exist for implementing HALT and HASS, tailoring is needed on each item and application. HALT and HASS are focused on detecting and eliminating failure modes at the component and sub-component level so that corrective action can be taken.

Highly Accelerated Life Testing (HALT). HALT is an activity implemented along with design verification tests that are planned and conducted during the design and development process. HALT is not a compliance test and does not replace qualification testing requirements. HALT, which is part of an overall comprehensive T&E program, will quickly reveal failure modes that would/could occur during the life of the product under normal operating conditions.

HALT is a form of accelerated testing used to determine whether the item (e.g., components, sub-components) can withstand environmental stresses. Early in the design and development processes, HALT is conducted in a specialized environmental chamber to expose items to a full range of operating conditions. During HALT, environmental stresses are controlled and incrementally applied until they eventually reach a level beyond that which is expected during operational use. Stresses applied during HALT are typically temperature and/or vibration; however, other stresses, such as electrical or mechanical, are also considered. HALT, utilizing combinations of these stresses, is recommended to emulate real-world conditions.

Exposing items to environmental stresses forces failures in order to understand operational margins and identify weaknesses in the design that need corrective actions. If the item (component or sub-component) survives HALT, it passes the test. Any deficiencies identified during HALT are inspected and analyzed to guide refinement of the design and elimination of the cause(s) of failure.

Reliability growth testing (RGT) is conducted in parallel with HALT to provide engineering confirmation and feedback. Information captured from previous testing and analysis is used to ensure that any areas of concern are properly instrumented and tracked for future tests. Corrective actions are taken to mitigate the reliability deficiencies that arise during testing. Examples of corrective actions include engineering redesign of mechanical components, software recoding, and adjustments to training practices.

After the corrective actions are in place, accelerated tests can also be used to quickly verify the corrective actions. Dynamic M&S, finite element stress and heat transfer analysis, and component fatigue analysis toolsets are some of the methods utilized to predict failure mechanisms and support reliability assessments of the proposed design and any subsequent design revisions.

Highly Accelerated Stress Screening (HASS). HASS is discovery testing as compared to compliance testing. HASS identifies inferior/defective items by exposing the production item to accelerated stresses to identify defects early, before a large number of items with similar flaws are produced. HASS is implemented to ensure the reliability of production line products. HASS is one of several screening approaches used by the DoD/industry to provide the opportunity to substantially improve fielded product reliability and reduce overall cost of ownership.

HASS uses accelerated stresses (beyond the product specifications) on production items to identify latent and intermittent defects that are a result of a problem in the manufacturing process. The stresses applied during HASS are based on operational and destructive stress limits established during HALT. HASS is usually not recommended unless a comprehensive HALT has been performed.

CH 8–3.7.4 Scientific Test & Analysis Techniques

In accordance with DoDI 5000.02 (Encl. 4, para 5(a)(3) – page 67) and DoDI 5000.02 (Encl. 5, para 5(e) – page 71), T&E planning includes the use of Scientific Test and Analysis Techniques (STAT) to produce statistically defensible test results and effectively support decision-makers. STAT is defined as the scientific and statistical methods, with associated processes, used to enable the development of efficient, rigorous test strategies so as to yield defensible test results. STAT encompasses techniques such as design of experiments, observational studies, and survey design. The specific objective(s) of the test determines the suitability and specific application of each method.

STAT is applied to test design and analysis throughout all phases of the acquisition life cycle. Various types of test events (e.g., contractor, developmental, live fire, operational, cybersecurity, interoperability, and modeling and simulation) can utilize STAT to achieve defensible results. STAT enables estimation of technical performance requirements as well as the mission-oriented metrics of operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality over the entire operational envelope. Depending on the test goal, different STAT methods may apply. **Error! Reference source not found.**, provides some examples of what methods might apply at different test phases in a program's development, depending on the goal of the test.

Table 6: Linkage between STAT & Test Goals

Test Objective	Likely Applicable Test Phase	Potentially Useful Experimental Designs
Characterize performance across an operational envelope Determine whether a system meets requirements across a variety of operational conditions	DT and OT	Response surface designs, optimal designs, factorial designs, fractional factorial designs

Compare two or more systems across a variety of conditions	DT and OT	Factorial or fractional factorial designs, matched pairs optimal designs
Screen for important factors driving performance	CT and DT	Factorial or fractional factorial designs
Test for problem cases that degrade system performance	Primarily DT, OT for Business Systems	Combinatorial designs, Orthogonal Arrays, Space filling designs
Optimize system performance with respect to a set of conditions	CT and early DT	Response surface designs, optimal designs
Predict performance, reliability, or material properties at use conditions	CT and early DT	Response Surface Designs, Optimal Designs, Accelerated life tests
Improve system reliability or performance by determining robust system configurations	CT and early DT	Response surface designs, Taguchi designs (Robust Parameter Designs), Orthogonal Arrays

Note. DT = Developmental Test OT = Operational Test CT = Contractor Test.

The proper and early use of STAT produces tests yielding defensible results as well as answering the test objectives, identifying risks of making inaccurate conclusions, and reducing uncontrolled experimental error. A sequential testing approach allows test organizations to accumulate evidence of system performance across its operational envelope, thus leveraging information from previous tests. A statistical, scientifically based approach to testing also informs the systems engineering process, and enables a better understanding of the true state of technology and system performance throughout the acquisition life cycle.

A program applying STAT starts early in the acquisition process and assembles a team of subject matter experts to identify the primary evaluation metrics of interest against both the technical performance requirements, as well as the mission-oriented metrics that characterize the performance of the system and its capabilities in the context of a mission-oriented evaluation. The team identifies the factors, as well as the levels of these factors (i.e., the various conditions or settings that the factors can take), expected to drive the technical and operational performance of the system. The anticipated effects of each of the factors on the evaluation metrics are determined to aid in test planning. To maximize test efficiency, the team uses experimental design techniques to strategically vary factors across the various developmental, operational, and live fire test activities. The test design balances limited test resources with adequate coverage of the operational envelope, while minimizing test risks.

The TEMP outlines a brief overview of the test design philosophy and use of STAT. While the information content varies depending on which milestone the TEMP supports, the test design plan(s) reflect the complexity of the system. Often multiple test design plans are necessary to fully characterize the performance of the system under test. Besides factors and their levels, design details also include statistical measures of merit (including but not limited to power and confidence) on the relevant evaluation metrics. These statistical measures are important to understand "how much testing is enough," and they provide the decision-makers the quantitative basis to conduct trade-off analyses, and provide defensible measures of the test scope and needed resources. The merit of a test design is based not only on the number of test points, but also their placement within the operational envelope. The statistical measures of merit used to evaluate the statistical adequacy of the test design are consistent with the test goal. For example, if characterization of system performance across a variety of conditions is a test goal, then the

power calculations provide a measure of the ability of the test to detect differences in performance amongst the conditions of the test. A supporting appendix to the TEMP provides the details of each of the test designs.

The analysis of test data and reporting of test results employ STAT as well. If advanced experimental design methods are used to develop the most efficient test design and execution plan, but the analysis of the data does not take advantage of the principles that drive that design, then the benefits are lost. STAT enables the data from testing to provide the most information from the data for the fewest resources. The reporting of average performance across all conditions varied in the test, for example, is dissuaded; as such, analysis methods can miss identifying important performance shortfalls. Comprehensive statistical analyses are employed to take advantage of the efficiencies and increased information provided by a rigorous experimental design.

For more information on STAT, visit the STAT in T&E Center of Excellence (STAT COE).

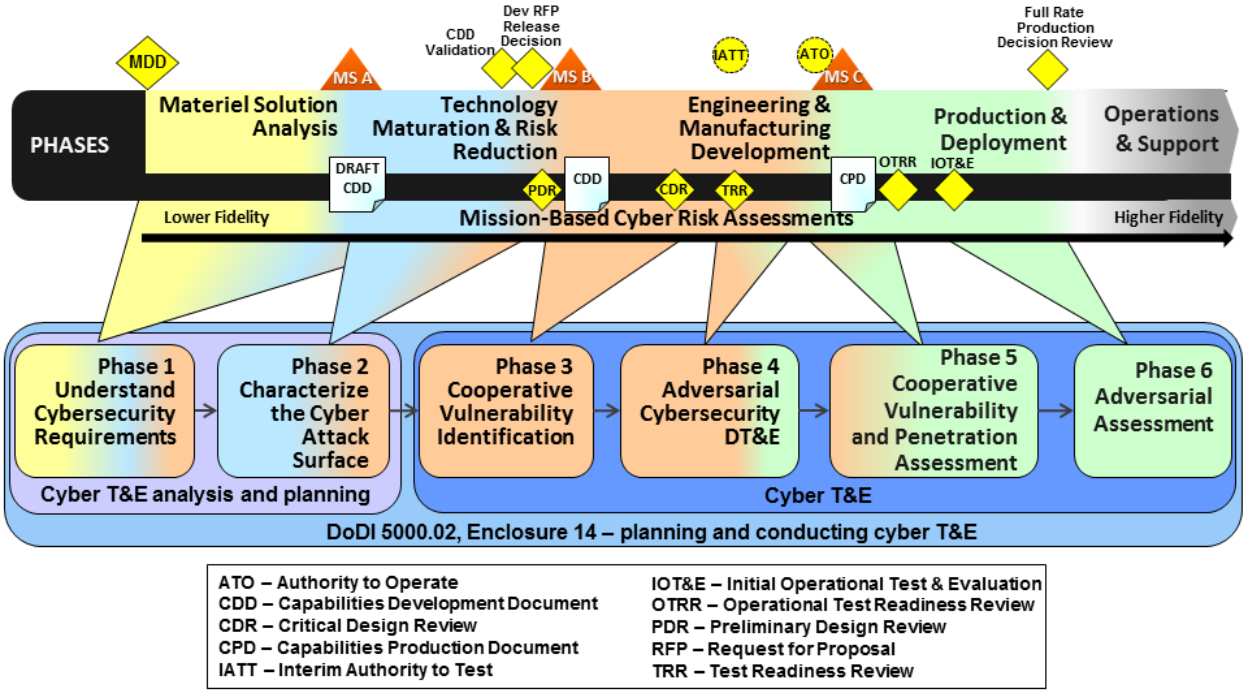
CH 8–3.7.5 Cybersecurity T&E

DoD missions depend upon complex, interconnected information technology (IT) environments. These environments are inherently vulnerable, providing opportunities for adversaries to negatively impact DoD missions. Addressing cybersecurity early in the acquisition process requires a comprehensive T&E program, which provides early discovery and allows for correction of developmental and operational issues, in support of the warfighter. The policy for Cybersecurity is defined in DoDI 5000.02 (Encl. 14 – page 155), Cybersecurity in the Defense Acquisition System.

This section provides an overview to assist the Chief Developmental Testers and the entire test community in developing an approach to cybersecurity T&E. Per DoDI 8500.01 (Para 3(h)(3) – page 4), developmental and operational testing are an integral part of implementing Cybersecurity in the system lifecycle. The instruction also defines “Operational Resiliency” and the requirement for performing developmental T&E of cybersecurity and OT&E to include “the ability to detect and react to penetrations and exploitations and to protect and restore data and information, in order to inform acquisition and fielding decisions” (Enclosure 3, Para 3.b – page 31). Cybersecurity T&E planning, analysis, and implementation is an iterative process starting at the beginning of the acquisition life cycle and continuing through maintenance of the system.

Figure 1 depicts the Cybersecurity T&E Process phases, occurring from pre-Milestone A test planning, through developmental test, to cybersecurity OT&E after Milestone C.

Figure 1: Cybersecurity T & E Process Mapped to the Acquisition Lifecycle



This figure presents a baseline mapping of the six Cybersecurity T&E process phases to the acquisition life cycle; the mapping of process phases may be tailored to the acquisition model used by the program, as defined in DoDI 5000.02 (Encl. 5, para 8 – page 73). The process should translate cybersecurity requirements, host environments, threats, and other considerations into testing. Early developmental T&E involvement in acquisition planning and execution remains a key feature of the cybersecurity T&E Process Additionally, programs can plan some phases to occur concurrently, depending upon when in the acquisition life cycle the program begins the process.

The Cybersecurity T&E process is iterative (i.e., programs may repeat phases several times throughout the acquisition life cycle, due to changes in system architecture, new or emerging threats, and changes to the system environment). For example, the first two phases, which involve analysis to understand requirements and define the cyber-attack surface, may be iterated with a major change to the system architecture. These activities would be coincident with updates to the TEMP and with systems engineering activities to update requirements, architecture, and design.

It is recommended that the CDT establish, as early as possible, a Cybersecurity Working Group (CyWG) that reports to the T&E Working Integrated Product Team (WIPT). This group will help the CDT plan and carry-out the Cybersecurity T&E phase activities.

The six phases of developmental and operational test preparation and execution are described briefly in the following subsections. More detailed information can be found in the Cybersecurity T&E Guidebook.

CH 8–3.7.5.1 Understand Cybersecurity Requirements

Enclosure 14 of DoDI 5000.02, paragraph 5.b.(10), describes Phase 1 of cybersecurity T&E analysis that takes place during Materiel Solutions Analysis (MSA).

As early as possible in the acquisition process, the Chief Developmental Tester, in collaboration with the CyWG, should examine program documents (i.e., Acquisition Strategy, Cybersecurity Strategy, Capabilities Development Document (System Survivability KPP), and other system requirements documents) to gain an understanding of system cybersecurity requirements. The Chief Developmental Tester and CyWG should ensure system cybersecurity requirements are complete and testable. Based on the requirements review, the CyWG constructs a T&E strategy to address the cybersecurity requirements and threat profiles. This phase is performed iteratively, as system development proceeds.

For Joint programs, JCIDS documents should now specifically include cyber survivability attributes (requirements) pulled from the Cyber Survivability Implementation Guide. In addition to providing these cybersecurity attributes, this guide also explains how requirements writers will determine the Cyber Survivability Risk Category of the system. This categorization assesses the overall cyber risk to the system. The depth and breadth of cybersecurity testing should match the overall cyber risk to the system.

Note: Although the CSE is only required for capabilities with Joint interest, the Services are encouraged to use this guide for capability requirement documents that are validated by the DoD Component sponsor.

CH 8–3.7.5.2 Characterize the Cyber Attack Surface

Enclosure 14 of DoDI 5000.02 paragraph 5.c.(5) describes the Phase 2 analysis and collaboration that takes place during Technology Maturation and Risk Reduction.

The attack surface defines the system's exposure to reachable and exploitable vulnerabilities, including any hardware, software, connection, data exchange, service, removable media, wireless or Radio Frequency (RF) communications, etc., that might expose the system to potential threat access. The T&E WIPT, via the CyWG, should update the Milestone B (or relevant milestone) TEMP with plans for testing and evaluating the elements and interfaces of the system deemed susceptible to cyber threats.

Note: Program management documentation is essential to characterizing the attack surface. This documentation should include the system architectures, network diagrams, system engineering plans, program protection plans, and certification and accreditation artifacts.

CH 8–3.7.5.3 Cooperative Vulnerability Identification

Enclosure 14 of 5000.02 paragraph 3(a)13(a)(1) requires systems to conduct T&E activities to identify vulnerabilities.

The Chief Developmental Tester, in conjunction with the CyWG, defines vulnerability-type testing events for contractor and government cybersecurity testing at the component and subsystem level. This testing assists in refining the scope and objectives for subsequent cybersecurity T&E and is integrated to the greatest extent possible into the T&E program as a whole. Preparation for vulnerability identification events is performed, in part, by understanding the cybersecurity kill chain (which considers how an adversary might exploit vulnerabilities). The vulnerabilities identified in this and previous phases should be resolved or mitigated prior to proceeding to a full end-to-end DT&E assessment defined in the next activity. This phase is not a single test event. Phase 3 should be a continuum of testing informed by the analysis in Phases 1 and 2, MBCRAs and statistical analysis techniques to plan and scope the testing.

CH 8–3.7.5.4 Adversarial Cybersecurity Developmental T&E

Enclosure 14 of 5000.02 paragraph 3(a)13(a)(2) requires systems to conduct an Adversarial Cybersecurity DT&E event.

This phase serves as an end-to-end threat-based assessment in a representative mission context for the system under test in order to evaluate the readiness for limited procurement/deployment and operational testing. The cybersecurity DT&E assessment typically occurs before Milestone C. This activity focuses on conducting a rigorous cybersecurity test in an environment as realistic as available, and requires the use of a threat-representative test team that tests the potential and actual impacts to the system and the mission. For DT&E, the threat-representative test team does not have to be NSA certified as long as testing is not conducted on an operational network. Results of this testing are included as part of the DT&E Sufficiency Assessment. Programs should resolve any shortfalls identified in this and previous phases prior to proceeding to operational test and evaluation, and programs should plan sufficient time and resources for these resolutions.

CH 8–3.7.5.5 Cooperative Vulnerability & Penetration Assessment

Sections 3.7.5.5 and 3.7.5.6 discuss cybersecurity operational testing, which consists of two components: a Cooperative Vulnerability and Penetration Assessment, which is conducted in cooperation with the program manager, and an Adversarial Assessment, which emulates an actual adversary attack on the system and its associated network(s). Cybersecurity operational testing guidelines are provided in

DOT&E's memorandum, “Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs,” dated April 3, 2018. These two testing activities are also described in DoDI 5000.02, Enclosure 14 paragraphs 3(a)13(b)(1) and 3(a)13(b)(2).

This Cooperative Vulnerability and Penetration Assessment phase consists of an overt, cooperative, and comprehensive examination of the system to identify vulnerabilities and characterize the system’s operational cybersecurity status. A vulnerability assessment and penetration testing team should conduct this test event through document reviews, physical inspection, personnel interviews, and the use of automated scanning, password tests, and applicable exploitation tools. The assessment should be conducted in the intended operational environment, with representative operators to the greatest extent possible. This testing may be integrated with DT&E activities (or earlier in the acquisition cycle) if conducted in a realistic operational environment; and if approved by the Director of Operational Test and Evaluation for programs on DOT&E Oversight.

CH 8–3.7.5.6 Adversarial Assessment

This phase assesses the ability of a system to support its missions while withstanding validated and representative cyber threat activity. In addition to assessing the effect on mission execution, the test should evaluate the ability of the system to detect threat activity, react to threat activity, and restore mission effectiveness degraded or lost due to threat activity. This test event should be conducted by an operational test agency employing a certified adversarial team to act as a cyber-aggressor. The adversarial assessment should include representative operators and users, local and non-local cyber network defenders (including upper tier computer network defense providers), an operational network configuration, and a representative mission with expected network traffic.

CH 8–3.7.5.7 Mission-Based Cyber Risk Assessment (MBCRA)

Mission-Based Cyber Risk Assessments, such as a Cyber Table Tops, are used to identify, estimate, and prioritize risks to DoD operational missions resulting from cyber effects on the system(s) supporting those missions. MBCRAs can be an effective means of understanding cybersecurity requirements, evaluating cyber-attack surfaces, exploring mission effects from exploits of the attack surface, and planning cybersecurity test events. In addition to informing cybersecurity testing, these assessments align to the NIST 800-30 Risk Assessment Guide and can inform each step of the Risk Management Framework. MBCRA activities should start as the threat characterization is being developed and continue periodically throughout the system life cycle, updated any time the threat characterization is updated, and any time countermeasure evaluation or threat portrayal testing occurs to ensure that any changes to mission risk are captured. The program evaluates and updates the cyber risk assessment and the RMF risk assessment report if necessary using information from the updated threat assessment. MBCRAs should introduce and explore the effects of cyber-attacks to determine how they impact the ability of a system, System of Systems, or Family of Systems to execute a mission. MBCRAs:

- Identify potential threat vectors
- Identify risks associated with those threat vectors
- Categorize risk within the mission context
- Inform mitigations analysis, engineering, testing, and design activities

Typical systems will have many potential threat vectors and they cannot all be tested. MBCRAs can inform which vectors represent the greatest risk to the mission so that testing can be planned accordingly. More information on MBCRAs can be found in the Cybersecurity T&E Guidebook.

CH 8–3.7.5.8 Cybersecurity T&E Overarching Guidelines

Cybersecurity T&E overarching guidelines include:

- Test activities integrate Risk Management Framework (RMF) security controls assessments with tests of commonly exploited and emerging vulnerabilities early in the acquisition life cycle, during Phase 3, in accordance with DoDI 8500.01 (Encl. 2, para 3(c) – page 18). Refer to the DoD RMF Knowledge Service (DoD CAC required) for more information on RMF security controls, in accordance with DoDI 5000.02 (Encl. 4, para 4(b)(13) – page 66). The pursuit of an Authorization

to Operate (ATO) does not replace or negate the need to perform operational resiliency testing during DT&E and OT&E, as required in DoDI 8500.01.

- The TEMP details the ways testing provides the information needed to assess cybersecurity and inform acquisition decisions. Historically, TEMPs and associated test plans have not adequately addressed cybersecurity measures or resources. The process described here facilitates development and integration of cybersecurity T&E, including the use of specialized resources; and facilitates the documentation of cybersecurity T&E in the TEMP.
- Cybersecurity DT&E identifies issues related to resilience of military capabilities before Milestone C. Early discovery of system vulnerabilities can facilitate remediation to reduce impact on cost, schedule, and performance. DASD(DT&E) includes an evaluation of cybersecurity in Defense Acquisition Executive Summary (DAES) reviews and DT&E Sufficiency Assessments, provided at major decision points.
- Cybersecurity OT&E ensures the system under test can withstand realistic threat representative cyber-attacks and return to normal operations in the event of a cyber-attack. See the DOT&E memorandum, "Procedures for OT&E of Cybersecurity in Acquisition Programs," dated April 3, 2018.
- Cybersecurity T&E stakeholders are strongly encouraged to engage Service Operational Test Agencies early and often during the six phases. OTAs integrate developmental and operational testing, independent evaluations, and assessments to provide essential information to acquisition decision makers and commanders.
- The Cybersecurity T&E Process represents a "shift left" on the acquisition timeline because it requires earlier developmental T&E involvement.
- The Cybersecurity T&E process recommends the development and testing of mission-driven cybersecurity requirements, which may require specialized systems engineering and T&E expertise. The Chief Developmental Tester and/or operational test agency may request assistance from subject matter experts to implement this process.

Table 7: Cybersecurity Example Issues, provides some example issues programs may consider for inclusion in the Evaluation Framework, to be evaluated using DT and OT test events and resulting in a cybersecurity evaluation for the program:

Table 7: Cybersecurity Example Issues

Overarching Cybersecurity Developmental Issue	Can mission-critical cybersecurity assets withstand cyber-attacks and intrusions? Can the system adequately recover from cyber-attacks and intrusions?
Example Issue 1, Systems and Software Assurance	Is the system/software/hardware developed using industry security best practices?
Example Issue 2, RMF Requirements	Do security controls and countermeasures prevent and mitigate malicious activities as intended?
Example Issue 3, Vulnerability Assessment	Do exposed vulnerabilities adversely affect system resiliency?
Example Issue 4, System interoperability and functionality in response to exploited cyber vulnerabilities	Is the system sufficiently interoperable and able to sustain critical mission functions in response to exploited cyber vulnerabilities?

Refer to the Cybersecurity T&E Guidebook for additional information on cybersecurity T&E resources and an in-depth overview of the Cybersecurity T&E Process.

CH 8–3.7.6 Interoperability Testing of IT & NSS

All information technology (IT) and National Security Systems (NSS) must undergo interoperability T&E for certification prior to fielding, in accordance with:

- 10 USC 2223, Information Technology; additional responsibilities of Chief Information Officers.
- DoDI 5000.02 (Encl. 4, para 4(b)(14) – page 99 and Encl. 5, para 5(d)(4) – page 107), Operation of the Defense Acquisition System.
- DoDI 8330.01, Interoperability of Information Technology (IT), Including National Security Systems (NSS).
- CJCSI 3170.01I, Joint Capabilities Integration and Development System.

This includes IT and NSS compliance with technical standards, Net-Ready Key Performance Parameters (NR-KPP), Enterprise Architectures, and spectrum supportability requirements.

For IT/NSS with *Joint, multinational,* or *interagency* interoperability requirements: the Joint Staff certifies the NR-KPP and Joint Interoperability Test Command (JITC) tests and certifies the system against the NR-KPP (alternatively, programs can use another test organization to conduct the testing, but JITC must evaluate the results and make the interoperability determination).

For all other IT/NSS: the individual DoD Components certify the NR-KPP and test and certify the system against the NR-KPP.

Compliance with interoperability certification requirements must be maintained throughout a system's life cycle. In accordance with DoDI 8330.01 (Encl. 3, para 6(d)(2) – page 33), each system must be re-evaluated every four years to determine if it needs to be recertified. Independent of the four-year requirement, if system interoperability functionality or requirements change at any time, the system must be recertified.

Interoperability test certification is based on T&E results from system-of-systems events featuring execution of Joint Mission Threads in operationally realistic test configurations (including the cyber threat). Enterprise architectures are used to identify system interfaces and build operationally realistic environments. System-of-systems test events verify the system meets its interoperability requirements, including the three elements of the NR-KPP:

- Support military operations.
- Enter and be managed on the network.
- Effectively pass information.

NR-KPP attributes determine specific measurable and testable criteria for interoperability and operationally effective end-to-end information exchanges.

Per DoD 5000.02, approval for the MS C decision depends in part on specific criteria defined at Milestone B and included in the Milestone B ADM. One of the general criteria for the MS C decision is "demonstrated interoperability". Therefore, prior to executing comprehensive system-of-systems events, which frequently occur during operational testing (and after Milestone C) , programs can address two

aspects of the Net-Ready KPP (NR-KPP), "Enter and be managed on the network" and "Effectively pass information", with networking, connection, and data exchange test activities. These activities can take place earlier in the development process and can pinpoint issues at a time when they can be fixed more readily and less expensively. If possible, more comprehensive interoperability testing should take place in the later stages of developmental testing. For IT/NSS with Joint, multinational, or interagency interoperability requirements, JITC is directed to leverage previous, planned, and executed DT&E and OT&E test events, and their results to support Joint interoperability test certification and eliminate test duplication. It is important to involve JITC early in the test planning process so that they can set forth their requirements (test conditions, data collection) for accepting and using test data for interoperability certification. To achieve standardization and efficiencies, JITC and DoD Component stakeholders (i.e., PMs, DT organizations, OTAs) must employ a common evaluation framework for interoperability requirements analysis, test planning, execution, reporting, and subsequent certification.

The Chief Developmental Tester, in coordination with the Lead Developmental Test and Evaluation Organization, plans and programs (budget and resources) interoperability T&E activities and documents these activities in the TEMP. The plans included in the TEMP must describe the strategy for evaluating the NR-KPP and meeting interoperability certification requirements. To facilitate T&E planning in the TEMP, the Chief Developmental Tester should look for the NP-KPP and Enterprise Architectures to be available, at least in draft versions, prior to or at MS B. Interoperability measures and events should be included in the overarching Developmental Evaluation Framework. For programs with Joint, multinational, or interagency interoperability requirements, Chief Developmental Testers should include JITC as a member of the T&E WIPT, and JITC should be identified as a participating test organization with the lead developmental test and evaluation organization. JITC should ensure they participate in TEMP development through the leader developmental test and evaluation office (this helps ensure that JITC can leverage the data collected during DT).

The appropriate DT&E authority approves TEMPs, or equivalent documents, for each ACAT program after verifying that adequate levels of DT&E to achieve interoperability certification are planned, resourced, and can be executed in a timely manner.

The DT&E Sufficiency Assessments at Milestones B and C will include a review of interoperability. At MS B the assessment will concentrate on the adequacy of planned interoperability testing. The MS C assessment will concentrate on the sufficiency of completed interoperability testing, interoperability risks identified during that testing, and the plans for remaining interoperability testing.

Considerations for the MS A TEMP:

- Understand T&E Implications of interoperability requirements in the Capabilities Development Document (CDD), System Requirements Documents, ICD, Draft Information Support Plan (ISP), etc.
- Key information exchange architectures (system, network) are identified as well as the data to be exchanged. This includes DODAF Operational Viewpoints (OVs), Services Viewpoints (SvcV), Technical Standards (StdV)
- OMS/MP or CONOPs is reviewed to understand intended use
- Program Protection Plan is reviewed to understand critical functions and components
- Critical interfaces and mission threads that support military operations are identified
- Test resource requirements (including the testing environment) are identified
- T&E Strategy describes
    - The overall approach to mitigate interoperability risks
    - Methods of testing key interfaces, functions, and mission threads
    - The DT&E approach for interoperability (if possible, include Developmental Evaluation Framework), including infrastructure, data, and services interoperability
    - Timelines

At PDR:

- T&E WIPT or subgroup reviews interoperability requirements
- Feedback is provided to the program on interoperability requirements and whether they are measurable, testable, and achievable

Considerations for the MS B TEMP:

- T&E Strategy that describes DT&E for infrastructure, data, and services interoperability in as close to a mission environment as possible (i.e. systems-of systems, etc.)
- Developmental Evaluation Framework (DEF) defines required data needed for interoperability evaluations and the test events that will supply that data
- Test resources for interoperability events are documented (e.g. Facilities, People, Test Environment, Funding, etc.)
- Plans to obtain an Interim Authorization To Test (IATT) are documented (post CDR) (demonstrate interoperability prior to MS C)
- The Draft Milestone B TEMP is used as a source document when developing the Engineering & Manufacturing Development (EMP) RFP
    - Ensure contractor T&E activities and deliverables are included
    - Ensure alignment between TEMP and ISP at RFP Decision Point
    - Use the ISP to validate RFP requirements for T&E and inform government T&E planning

At CDR:

- Testing should match limitations and critical information requirements in the interface control documents
- Consider interoperability requirements in a system of systems environment, including infrastructure, data, services, and threat actors
- T&E WIPT provides feedback on testing to date and on future testing plans, to include T&E in a mission context using OMS/MP or CONOPs

EMD:

- Assemble the mission representative test environment and test architecture for system level (and system-of systems) interoperability testing (e.g., Live-Virtual-Constructive)
    - NR KPP - demonstrate ability to enter and be managed on the network, effectively exchange information, and support military operations
- Obtain IATT to support demonstration of interoperability prior to MS C
- Demonstrate the critical operational missions (i.e. OV-6C) in a representative environment involving multiple systems

JITC Interoperability Process Guide (IPG)—For those programs with Joint, multinational, or interagency interoperability requirements, JITC has developed and published an Interoperability Process Guide (IPG), in coordination with the DoD CIO, Outline the procedures and documentation required for Joint Interoperability Test and Certification, waiver processing, and other associated processes and procedures.

Interoperability Test Resources—The TRMC's JMETC Program provides a DoD-wide capability for distributed T&E. (See DAG, CH 2.2.3.3., Joint Mission Environment Test Capability for more information.) In addition, JITC offers a suite of customized tools that track a system's lifecycle through the phases of the Joint Interoperability Test and Certification process. These tools allow for the push-button creation of traceability matrices and test planning documentation, quantitative and qualitative data analysis, and enhanced reporting capabilities (see the JITC Homepage for more information).

Refer to the DAG, CH 6.3.8. for more information on Interoperability.

CH 8–3.7.7 Modeling & Simulation in T&E

This section provides information on the use of modeling and simulations in test and evaluation. Programs should identify the appropriate use of modeling and simulation for each test phase or event, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(10) – page 68) and (Encl. 5, para 6(d) – page 72).

CH 8–3.7.7.1 Modeling & Simulation Purpose & Application

Models and simulations are valuable in determining how to apply scarce test resources to high-payoff areas, help identify cost-effective test scenarios, and reduce risk of failure. During the conduct of tests, models, simulations, and digital artifacts can create realistic developmental and operational test scenarios and objectives; provide virtual environments to dry run test events; and provide testers the ability to conduct tests where the use of real-world assets is deemed impractical or costly. This may occur as part of system-of-systems tests, under hazardous/dangerous conditions, or in extreme environments. Programs can use models, simulations, and digital artifacts in post-test analysis to help provide insight and for interpolation or extrapolation of results to untested conditions.

Models and simulations provide programs with different tools as follows:

> Model: A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process.
>
> Simulation: A method for implementing a model over time.

The use of models, simulations, and digital artifacts provides a means to understand the risks associated with technical development and operational employment of a system. The PM must balance programmatic needs to better understand these risks with the cost and time required to obtain credible and trusted models, simulations, and digital artifacts to support the necessary capability. T&E often reveals “unknown unknowns” in system development and planned use, especially in live fire and operational environments. Whenever feasible, observation of system performance and the use of empirical data from testing are the most credible means to evaluate system performance.

Similarly, the Chief Developmental Tester and operational testers balance their needs to address the risks encountered in DT&E, OT&E, and LFT&E with the cost and time required to acquire and use adequate and credible model and simulation capabilities. Models, simulations, and digital artifacts can be used to support test planning, execution, and evaluation of test results. When models, simulations, and digital artifacts are needed to support T&E, the program plans for and funds the development for this capability. Validation efforts typically involve the collection of live data to provide the necessary information upon which to base the VV&A; and those efforts are planned and funded.

Programs plan for models, simulations, and digital artifacts for utility across a program’s life cycle, modified and updated as required, to ensure use in and applicability to all increments of an evolutionary acquisition strategy. A program's T&E strategy leverages the advantages of models and simulations. Models, simulations, and digital artifacts planning addresses which of many possible uses of models, simulations, and digital artifacts the program plans to execute in support of T&E, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(5) – page 67).

Evaluators use a model-test-fix-model approach for interaction of T&E and modeling and simulation. This iterative process provides a cost-effective method for overcoming limitations and constraints upon T&E.

Refer to the DoD Modeling & Simulation Coordination Office (MSCO) for more information on applications of models, simulations, and digital artifacts considerations.

CH 8–3.7.7.2 Modeling & Simulation Processes & Implementation

All models and simulations used in T&E come from an authoritative source and are accredited by the intended user (PM or OTA). Programs can only receive accreditation through a rigorous VV&A process as well as an acknowledged acceptance by the user of their application requirements and documented in the TEMP, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(5) – page 67). Therefore, PMs identify the intended use of models and simulations early so they can make resources available to support development and VV&A of these tools. PMs also include the OTA early in their processes to gain confidence in the use of authoritative models and simulations, and possibly use of them in support of OT, in accordance with DoDI 5000.02 (Encl. 5, para 6(d) – page 72). When modeling and simulation tools are used as part of operational testing, the OTA independently accredits the tool.

T&E WIPT planning incorporates modeling and simulation into the overall T&E strategy (e.g., the employment of models and simulations in early designs, the use of models and simulations to demonstrate system integration risks, and the use of models and simulations to assist in planning the scope of live tests).

DT&E, OT&E, and LFT&E commonly integrate and use Live, Virtual, Constructive (LVC) capabilities and environments in T&E facilities and resources at open air ranges, system integration laboratories, installed system test facilities, and hardware-in-the-loop facilities. Credible modeling and simulation capabilities help to inform decision-making on system functionality, operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality, and operational security.

CH 8–3.7.7.3 Modeling & Simulation Policy & Guidance

Guidelines and instructions for the development and use of modeling and simulation (M&S) in acquisition are available from a variety of sources. Each program develops a modeling and simulation strategy to support overall program investments in modeling and simulation.

The Modeling and Simulation Coordination Office (M&SCO) Modeling and Simulation Catalog (DoD CAC required) is a user-friendly, web-based tool to collect M&S summary information and data, and provides a search capability to discover M&S resources for potential reuse and cost savings. The M&S Catalog is analogous to a “card catalog” (e.g., it assists in the discovery of resources, but does not generally contain the model or simulation code). For more information on the Modeling and Simulation Community of Interest Discovery Metadata Specification (MSC-DMS) and the M&S Community of Interest, see the M&SCO website.

Modeling and simulation products, and the manner of VV&A and other processes, conform to standards—both government and commercial. For example:

- IT standards identified in the DoD IT Standards Registry (DISR) (DoD CAC required).
- Standards identified in the DoD Architecture Framework Technical Standards Profile (TV-1) and Technical Standards Forecast (TV-2).
- ASSIST (DoD CAC required) is the official source for specifications and standards used by the DoD.
- Data standards.
- DoDI 5000.61, DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A), provides further guidance on VV&A.
- VV&A standards:
  - IEEE Std 1516.4-2007, IEEE Recommended Practice for VV&A of a Federation—An Overlay to the High Level Architecture Federation Development and Execution Process
  - IEEE Std 1278.4-2003, IEEE Recommended Practice for Distributed Interactive Simulation - VV&A.
  - DoD VV&A Recommended Practices Guide (RPG).
  - MIL-STD-3022, Documentation of Verification, Validation, and Accreditation (VV&A) for Models and Simulations.

Refer to the DAG, CH 3.2.4.2., DOT&E's Guidance on the Validation of Models and Simulation used in Operational Test and Live Fire Assessments, and DoDD 5000.59, DoD Modeling and Simulation (M&S) Management, for more information and guidance on modeling and simulation.

CH 8–3.8 Technical Reviews Supported by T&E

This section provides information on additional technical reviews supported by the test community, in accordance with DoDI 5000.02 (Encl. 3, para 7 – page 60). The test community also supports engineering reviews as described in DAG CH 3.3.3., such as System Requirements Review (SRR), Preliminary Design Review (PDR), Critical Design Review (CDR), etc.

CH 8–3.8.1 Technology Readiness Assessments

A Technology Readiness Assessment (TRA) is a systematic, metrics-based process assessing the maturity of, and the risk associated with, critical technologies to be used in MDAPs. The PM conducts the TRA with the assistance of an independent team of subject matter experts (SMEs). TRAs are a statutory requirement for MDAPs and a regulatory information requirement for all other acquisition programs, in accordance with DoDI 5000.02 (Encl. 1, Table 2 – page 38). The program may conduct a TRA concurrently with other technical reviews (see DAG, CH 3, Systems Engineering).

A preliminary assessment is due for the Development RFP Release Decision. The Assistant Secretary of Defense (Research and Engineering) (ASD(R&E)) conducts an independent review and assessment of the TRA conducted by the PM and other factors to determine whether the technology in the program has been demonstrated in a relevant environment.

Public Law 113-291 requires that the ASD(R&E), in consultation with the DASD(DT&E), shall submit to the Secretary of Defense and to the congressional defense committees by March 1 of each year, a report on the technological maturity and integration risk of critical technologies of the major defense acquisition programs of the DoD. DASD(DT&E), in consultation with ASD(R&E), assesses the technologies at key stages in the acquisition process, in accordance with DoDI 5134.17 (Encl. 2, para e).

The Chief Developmental Tester, upon consultation with the Lead DT&E Organization and the T&E WIPT, participates and assists in the assessment of the technologies.

Refer to 10 USC 2366b for more information.

CH 8–3.8.2 Preliminary Design Review

The PDR should provide sufficient confidence to proceed with detailed design. It ensures the preliminary design and basic system architecture are complete, that there is technical confidence the capability need can be satisfied within cost and schedule goals, and that risks have been identified and mitigation plans established. The PDR provides the acquisition community, end user, and other stakeholders with an opportunity to understand the trade studies conducted during the preliminary design, and thus confirm that design decisions are consistent with the user's performance and schedule needs prior to formal validation of the Capability Development Document (CDD). The PDR also establishes the allocated baseline.

In accordance with DoDI 5000.02 (Para 5(d)(4)(g)(1)(b) – page 17), the PM supports T&E planning by finalizing sustainment requirements to support the PDR. The Chief Developmental Tester and the Lead DT&E Organization participate in the PDR and provide any analysis and assessments to date, as needed. During the TMRR Phase, and unless waived by the MDA, a PDR is conducted so it occurs before Milestone B and prior to contract award for EMD. The results from the PDR are used to help define entrance criteria for Milestone B and support the Development RFP Release Decision.

Refer to the DAG, CH 3.3.4. for more information.

CH 8–3.8.3 Critical Design Review

The Critical Design Review (CDR) assesses design maturity, design build-to or code-to documentation, and remaining risks, and establishes the initial product baseline, in accordance with DoDI 5000.02 (Encl. 3, para 7(b)(2) – page 60). The CDR serves as the decision point identifying the system design is ready to begin developmental prototype hardware fabrication and/or software coding with acceptable risk. The system CDR occurs during the EMD phase.

Besides establishing the initial product baseline for the system and its constituent system elements, the CDR also establishes requirements and system interfaces for enabling system elements such as support equipment, training system, maintenance, and data systems. The CDR should establish an accurate basis to assess remaining risk and identify new opportunities.

The Chief Developmental Tester and the Lead DT&E Organization participate in the CDR and provide any analysis and assessments to date.

Refer to the DAG, CH 3.3.5 for more information.

CH 8–3.9 Test Reviews

Test reviews are required prior to the execution of test events (whether by phase or key test event, etc.), as appropriate for the program, and documented within the TEMP. DoDI 5000.02 (Encl. 4, para 5(a)(4) – page 67), states that "each major developmental test phase or event will have test entrance and exit criteria." Although there are numerous and different types of test events, there are basic tenets that apply.

CH 8–3.9.1 Test Readiness Reviews

A Test Readiness Review (TRR) provides the formal approval authority with a review showing that the system is ready to enter the test and that the funding and execution of a test executes the test and gathers the required information. TRRs assess test objectives, test methods and procedures, test scope, safety, and whether test resources have been properly identified and coordinated. TRRs are also intended to determine if any changes are required in planning, resources, training, equipment, or timing to successfully proceed with the test. If any of these items are not ready, senior leadership may decide to proceed with the test and accept the risk, or mitigate the risk in some manner. A TRR is conducted for those events identified in the TEMP, in accordance with DoDI 5000.02 (Encl. 4, para 6(a) – page 68).

Documentation. TRRs are annotated within the TEMP on the integrated test program schedule. For more information, see Part 2.5 of the DAG, CH 8.3.6., Test & Evaluation Master Plan. TRRs need to include entry/exit criteria, which the Chief Developmental Tester, with the T&E WIPT, proposes to the PM for approval.

Composition. The PM or Chief Developmental Tester chairs the TRR, which generally consists of the following subject matter experts:

- Program Manager
- Chief Developmental Tester
- Program Systems Engineer
- Logistician
- Safety
- Lead DT&E Organization representative
- OTA Representative (as required)
- Test Facility/Range Representative (as required)
- DoD Component T&E Representative (as required)
- DASD(DT&E) Representative (as required)
- DOT&E Representative (if on oversight)
- Other SMEs (e.g., intelligence, cybersecurity, Trainer, etc.)

- Combat Developer/Tactics Developer/Fleet User.

CH 8–3.9.2 Operational Test Readiness Reviews

The OTRR is the formal approval process for deciding if a system is ready to enter operational testing, In accordance with DoDI 5000.02 (Encl. 5, para 12 – page 77). OTRRs are conducted to:

- Verify required contractor and/or developmental testing is complete with satisfactory system performance.
- Ensure OT test plans are approved and OT preparations are complete.
- Ensure other requirements supporting OT—such as threat representation validation reports and OTA accreditation of threat representations, models, simulations, and other test instrumentation—are complete.
- Verify that T&E and system under test resources and capabilities are available and ready to proceed with the OT&E.
- Verify system-under-test is production representative.
- Determine if any changes are required in planning, resources, training, equipment, or schedule in order to successfully execute the test.
- Identify any problems that impact on the start or adequate execution of the test and subsequent evaluation or assessment of the system.
- Make decisions as appropriate to resolve problems or to change or confirm scheduled requirements.
- Safety planning.

Schedule. DoD Components have internal processes for completing OTRRs. In general, the T&E WIPT initiates the process several months prior to convening the OTRR and oversees OT preparations and resolution of issues.

Composition. The OTA or responsible test organization chairs the OTRR. OTRR participants include:

- Program Manager
- Chief Developmental Tester
- Program Systems Engineer
- Sponsor
- Combat Developer/Capability Developer/Tactics Developer/Fleet User
- Logistician
- Safety
- Lead DT&E Organization Representative
- OTA Representative
- Test Facility/Range Representative (as required)
- DoD Component T&E Representative (as required)
- DASD(DT&E) Representative (as required)
- DOT&E Representative (if on oversight)
- Other SMEs (e.g., cybersecurity, trainer, etc.).

CH 8–3.10 Certifications

Certifications provide a formal acknowledgment by an approval authority that a system or program meets specific requirements. Certifications, in many cases, are based on statute or regulations and drive systems engineering (SE) planning (i.e., a program may not be able to test or field the capability without certain certifications). Used throughout the acquisition life cycle, certifications reduce program risk and

increase understanding of the system. Certain specific certifications are required before additional design, integration, network access, or testing can take place (e.g., Airworthiness certifications need to be in place before an aircraft can begin operations). Often programs insufficiently plan for the number of required certifications. Insufficient planning for certifications can have a negative impact on program costs and schedule.

Refer to the DAG, CH 3.2.6. for more information on certifications.

The system under development may require certifications, and the Chief Developmental Tester, in collaboration with the T&E WIPT needs to review the CDD to better ascertain the types of certifications required. Once identified, the TEMP includes the appropriate T&E and reporting to support the requisite certifications.

Examples of Certifications include:

- 2366a/2366b Certification Memorandum, in accordance with DoDI 5000.02 (Encl.1, Table 2 – page 31).
- Interim Authority to Test (IATT)
- Authorization to Operate (ATO)
- Safety (either for government/military test organizations or operational users)
- Interoperability
- Airworthiness
- Seaworthiness
- Food and Drug Administration (FDA)
- National Institute for Occupational Safety and Health (NIOSH)
- Environmental Compliance.

CH 8–3.10.1 Unified Capabilities Testing & Certification

DoDI 8100.04 (Glossary – page 26) defines Unified Capabilities (UC) as the integration of voice, video, and data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities. UC integrates standards-based communication and collaboration services including, but not limited to: messaging; voice, video, and web conferencing; unified communication; and collaboration applications or clients. These standards-based UC services must integrate with available enterprise applications, both business and warfighting.

The Unified Capabilities Certification Office (UCCO) manages the DoD UC-approved products list, providing guidance, coordination, and information to vendors and government sponsors throughout the entire process. The Unified Capabilities Requirements 2013 (UCR 2013) specifies the technical requirements for certification of approved products to be used in DoD networks to provide end-to-end UC. The UCR 2013 is the governing requirements document for all DoD network infrastructures and services that provide or support UC end-to-end; it takes precedence over subordinate documents, DoD standards, and commercial standards addressing UC. The UCR 2013 can be accessed via the DISA Approved Product List (APL) Process Guide page.

To achieve affordable, responsive, and efficient testing and certification of UC products for DoD Components, a distributed test concept was implemented. In accordance with DoDI 8100.04 (Encl. 2, para 2 – page 9), DISA/JITC serves as the primary test lab for the Defense Information Systems Network (DISN) and serves as the interoperability certification authority for all UC core products. Additionally, the Military Department (MILDEP) labs shall serve as the primary test labs for UC products that MILDEPs acquire and deploy at Base/Camp/Post/Stations and within tactical systems. UC Distributed Testing facilities include:

- DISA Joint Interoperability Test Command (JITC), Fort Huachuca, AZ
- DISA Joint Interoperability Test Command (JITC), Fort Meade, MD
- USAF Telecommunication Systems Security Assessment Program (TSSAP), San Antonio, TX
- Navy Space and Naval Warfare Systems Command (SPAWAR) Systems Center Atlantic, Portsmouth, VA
- Army Information Systems Engineering Command Technology Integration Center (TIC), Fort Huachuca, AZ

JITC develops UC test plans and formats for reporting results for all labs. The MILDEPs provide the results of UC testing to JITC for interoperability certification. The MILDEPs and JITC provide the results of UC Cybersecurity testing to DISA for Cybersecurity recommendations. The MILDEP Authorizing Official (AO) provides product and site accreditation for the installed UC products. In accordance with DoDI 8100.04 (Encl. 3, para 5(c)(5) – page 20), the DoD sponsor or the vendor shall be responsible for funding the testing and certification of UC products.

CH 8–3.10.2 Unified Capabilities Approved Products List

The Interoperability Certification and Cybersecurity Accreditation processes are applied to all UC product categories identified in the UCR 2013. The UCR 2013 defines the requirements that must be met for those products to be placed on the UC APL. The UC APL Process Guide defines the process by which UC and technology insertion products gain APL status.

For more information on UC and the APL, refer to the UC APL Process Guide and the UC APL (DoD CAC required).

CH 8–3.11 Developmental T&E Program Assessment

The DASD(DT&E) conducts DT&E Program Assessments for all MDAPs, MAIS, and programs designated as AT&L Special Interest programs, in accordance with DoDI 5000.02 (Encl. 4, para 6(b) – page 68). DT&E Program Assessments are completed at the Development RFP Release Decision Point, Milestones B and C, and updated to support the Operational Test Readiness Review (OTRR) or as requested by the MDA or PM. The MDA considers the results of the DT&E Program Assessment prior to making the Milestone Decision.

For MDAPs, MAIS programs, and USD(AT&L)-designated special interest programs, the DASD(DT&E) will provide the MDA with a program assessment at the Development RFP Release Decision Point, Milestones B and C, and updates thereafter to support the OTRR or as requested by the MDA or program manager. The program assessment will be based on the completed DT&E and any Operational T&E activities completed to date, and will address the adequacy of the program planning, the implications of testing results to date, and the risks to successfully meeting the goals of the remaining T&E events in the program.

For those programs not on DASD(DT&E) program engagement, the DoD Component assessment process includes a review of DT&E results, an assessment of the system's progress against the KPPs, KSAs, and CTPs in the TEMP; an analysis of identified technical risks to verify that those risks have been retired or mitigated to the extent possible during developmental testing; and a review of system certifications.

The DT&E Program Assessment for Development RFP Release Decision Point and Milestone B concentrates on:

- Plans
- Schedules
- Resources

- Additional Items (e.g., competitive prototyping, etc.)
- Recommendations.

The DT&E Program Assessment for Milestone C concentrates on:

- Adequacy of DT&E Planning
- Performance
- Reliability
- Interoperability
- Cybersecurity
- Recommendations.

DT&E Program Assessments are updated prior to IOT&E, as needed. DT&E Program Assessments can be performed at any time during the acquisition life cycle, if requested by the MDA or PM.

CH 8–3.12 Incorporating T&E into DoD Acquisition Contracts

Programs involve T&E personnel early and keep them involved with the PM, the KO, the SE, and the other program office leads throughout the contracting process, to ensure they understand, accept, and include T&E policies, practices, procedures, and requirements in the contract as necessary for program success, in accordance with DoDI 5000.02 (Encl. 4, para 4(b)(15) – page 66). Inputs from the Chief Developmental Tester, advised by the Lead DT&E Organization and the T&E WIPT, inform the contracting process on:

- The quantities, configurations, and types of deliverable test articles (expendable and non-expendable) and prototypes (if applicable) required for government T&E.
- Required contractor investments, expenditures, and developments required to support government T&E; e.g., threat simulators, targets, instrumentation, logistics and transportation for test preparation and set-ups, training, documentation, and personnel to support test events.
- Personnel and other support to T&E WIPT, integrated test teams.
- Contractor generated data and test reports for inclusion in the Contract Data Requirements List (CDRL).

In the early phases of development, the contractor plans and executes the majority of design testing that transitions technology from science and technology efforts into functional capabilities desired by the military, as well as qualification testing of sub-component parts and products from vendors that makes up the system delivered to the military. The Lead DT&E Organization and Participating Test Organizations need to understand the contractor testing capabilities, processes, data collection, and analysis methods to assess the appropriate amount of visibility into those test activities as well as determine data collection and transfer benefiting government test organizations to avoid redundant or unnecessary testing. Government test organizations determine cost/benefit ratios with visibility into proprietary activity and data transfer to the government. In addition, consideration is given to near- and end-state evaluations during operational testing (OT).

The PM, combat developer, and appropriate T&E personnel collaboratively develop the acquisition and T&E strategies so that users' capability-based operational requirements (i.e., CDD, Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP) are correctly translated into accurate contractual terms; and actions that give the highest probability of successful outcome for the government-contracted events provide for sufficient time to execute all regulatory and statutory T&E activities and reporting.

Incorporating T&E into DoD acquisition contracts is the test focus for the pre-RFP Review. It is essential that a good draft TEMP be available for the review and that the RFP adequately addresses the TEMP.

One key issue to remember: if the contract does not include a T&E item or requirement, *do not expect it!*

Refer to "Incorporating T&E into DoD Acquisition Contracts" for more information.

CH 8–3.13 Embedded Instrumentation

Embedded instrumentation is used to facilitate T&E data collection needs for measuring performance attributes and system diagnostics for debugging and failure analyses in an operational configuration (i.e., without having to change intended operational configuration to install additional instrumentation for testing). Operational Test Agencies (OTAs) should consider embedded instrumentation as their first choice for instrumented data collection. Embedded instrumentation requires independent accreditation and certification prior to use in OT&E. Also, embedded instrumentation could be optimized for facilitating training, logistics, and post-operational mission analysis and debrief.

Embedded instrumentation reduces the cost and complexity of adding additional instrumentation for the sole purpose of testing. While there is a cost for embedding instrumentation, the Chief Developmental Tester works with the logistician and trainer to share the costs and benefits of embedded instrumentation, as described above.

Sometimes, the developer has undocumented logs, ports, or tap points used during development for taking measurements. The Chief Developmental Tester looks for data products and rights to utilize this already planned instrumentation. Embedded instrumentation may include on-board data sensing and collection, storage, and/or real-time data transmission.

In accordance with DoDI 5000.02 (Encl. 4, para 5(a)(2)(d) – page 67), the PM, in coordination with the Chief Developmental Tester, ensures the program RFP includes any proposed use/application of embedded instrumentation, contractor involvement, and government oversight.

CH 8–3.14 Distributed Testing

Many of the capabilities used in, or to support, T&E are discussed in this chapter. These include land- or sea-based test facilities, legacy systems, new developments, threat systems, prototypes, etc. Also, the use of modeling and simulation is commonplace, which can be Live, Virtual, or Constructive (LVC). LVC capabilities can be integrated to provide Hardware-in-the-Loop (HITL or HWIL) or Systems Integration Laboratories, which can be used to support a T&E event. The majority of these T&E capabilities can be connected or linked.

In many cases, this is done with systems and capabilities that are not co-located so a distributed environment is developed to support the T&E event, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(6) – page 67). By sharing information through a Wide-Area Network (WAN) infrastructure, T&E capabilities can be linked across a test facility, across a T&E range, or around the world to form a distributed environment. Distributed Testing can be considered a process for linking various geographically separated LVC sites and capabilities together in a distributed environment; for use across the acquisition life cycle, to support and conduct the T&E of a subsystem, system, or system-of-systems (SoS) in a Joint or cyberspace environment.

Distributed Testing can be used to integrate systems and subsystems still under development as well as mature systems that already exist, but are located at geographically separated facilities. It can also be used to complement, or in some cases in lieu of, large-scale open air tests using actual operational hardware for the systems involved. Conducting Distributed Testing complements live-only testing and provides the means for rapid integration of components and systems early in a product's developmental life cycle. It also provides an efficient means of adding realism to T&E by providing systems and capabilities not otherwise available, or by including separate but interrelated systems and subsystems.

Conducting T&E by integrating components and capabilities early in a product's developmental life cycle reduces the technical risk of components not working together. Complementing the risk reduction inherent in early Distributed Testing, is the cost savings of correcting technical deficiencies before they become part of the operational design.

While Distributed Testing is particularly suited for many T&E activities, such as assessing a data exchange between components, subsystems, systems, or within a SoS, distributed methodologies are not appropriate for all T&E. For example, Distributed Testing would not be appropriate for system performance testing, reliability testing, and other tests that do not include other systems or systems-of-systems. However, PMs and Operational Test Agencies may consider Distributed Testing in situations where necessary systems, components, or capabilities are not co-located in a central test site. Also, Distributed Testing methodologies are considered when a system is required to demonstrate interoperability, which is the capability to work effectively with other systems. PMs tasked with conducting cybersecurity T&E consider the benefits of Distributed Testing methodologies, which provide the needed infrastructure and capabilities.

The advantages realized by Distributed Testing include, but are not limited to:

- Integrated T&E – Allows test events to share a single test point or mission that can provide data to satisfy multiple objectives, without compromising the test objectives of either the DT or OT. Early identification of system and mission elements enables the development and execution of an efficient and effective DT/OT integration in the strategy for T&E. This allows an early "Operational Influence" into the developmental cycle, in accordance with DoDI 5000.02 (Encl. 5, para 11(a)(4) – page 75). If done correctly, the enhanced operational realism in DT&E provides greater opportunity for early identification of system design improvements, and may even change the course of system development. While Integrated T&E does not replace or eliminate the need for dedicated Initial Operational Test and Evaluation, as required by 10 USC 2399, Operational Test and Evaluation of Defense Acquisition Programs. The goal is to conduct a seamless test program producing credible data to all evaluators that address developmental, operational, and sustainment issues early in the acquisition process—when the issues are easier and cheaper to correct.
- A near real-time Test-Fix-Test capability –That is, as a test event uncovers flaws in a system, the designers can make a correction and then immediately conduct a re-test to ensure the flaw has been fixed. This is especially true of software and information exchanges used in Command and Control systems.
- The ability of T&E Programs to "move data—not people" – The distributed nature of the event means that large teams of data collectors and analysts need not be deployed locally for the test event. Data collection and most analysis can be conducted from the home station with near real-time access to the needed test data.
- A collaborative, virtual workplace – Enables a connective relationship between geographically dispersed Subject Matter Experts (SMEs) and entities in the system-of-systems environment that they wouldn't have otherwise. This relationship can foster communication and feedback that can provide significant improvements to the systems under evaluation and across the spectrum of the mission area.

In recent years, the DoD has stood up a capability to provide a department-wide capability that makes Distributed Testing more accessible. The Joint Mission Environment Test Capability (JMETC) Program Office mission is to provide a DoD-wide capability for the T&E of warfighter capabilities in a Joint context for Interoperability, Key Performance Parameter (KPP) compliance testing, Developmental Testing (DT) and Operational Testing (OT), as well as Joint Mission Capability Portfolio testing.

Refer to JMETC for information on distributed testing.

CH 8–3.15 Threat Representation Evaluation

Beginning early in the acquisition life cycle, programs understand and monitor needs and requirements for threat representations to support testing since acquisition of intelligence information and physical assets can take significant time and resources, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(6) – page 67). For example, the identification of the need for surrogates in testing starts prior to Milestone A to ensure any needed changes or developments are understood early in the program. Validation and accreditation efforts of all surrogates used in operational testing begin no later than Milestone B, are ideally complete by Milestone B, and are documented in the TEMP, in accordance with DoDI 5000.02 (Encl. 5, para 10(c) – page 74). Regardless, threat representative validation and accreditation are completed prior to using any threat surrogate in operational and live fire tests.

"Threat representation" includes targets, models, simulations, simulators, emulators, stimulators, foreign materiel (that is, actual systems), U.S. equipment, and aerial, ground, sea-based, or other types of surrogates that portray specific foreign military weapon systems or civilian devices used in an adversarial military role. Scientific or technical equipment used to measure, sense, record, transmit, process, or display data during test or examination of materiel are not considered threat representative devices.

Threat Representation Validation. In order for the surrogate to be usable in a developmental or operational test, the surrogate is sufficiently representative of the threat(s) of interest to the fidelity necessary to accomplish the goals of the test. Threat representation validation is the process by which the users compare the key characteristics of the threat that are important to the performance of the system under test to those same key characteristics of the threat itself using DIA, DoD Component intelligence agency, and/or Service intelligence organization approved threat data. Validation includes quantifying the variations, and assessing the likely impact of those differences on the potential use of the threat representation for testing. The validation is a substantive and quantitative analysis conducted by a group of subject matter experts knowledgeable of the threat, as well as the system being tested, to select appropriate parameters and characterize the effects of any difference between the threat and surrogate parameters and operating characteristics and assess the impacts due to differences from the perspective of its intended use(s).

For target development, threat representation validation normally is conducted around two events in a threat representation's life cycle:

- Prior to initial operational capability (IOC) for the target.
- Whenever major modifications are made to the target or significant changes occur in the threat or its operational use.

Threat Representation Accreditation. Threat representation accreditation is the process used to determine whether threat representations are suitable for a specific test. Threat representation accreditation examines any parametric differences to determine their impacts on the test application and extend general information obtained during the validation process to a specific test application by analyzing and assessing its use and noting specific test limitations. The threat representation validation analysis provides sufficient evidence of the threat representation's operational status, permitting analysts to quickly understand its performance or contribution to an operational test event. Also, the data requirements are compared to the latest intelligence and the capabilities of threat representations as characterized by current validation efforts.

Accreditation decisions must be based on current assessments of the performance of the surrogate system for the following reasons:

- Any differences between a threat representation and the corresponding actual threat system can distort representation of the threat and affect the subsequent analysis of the system's effectiveness. Even the differences accepted during development and validation can make the

simulator/simulation or surrogate incapable of adequately representing the threat for a specific test application.

- The intelligence concerning threats is time-sensitive and dynamic. New intelligence can make a threat representation inappropriate for a given test application.
- Physical threat surrogates experience deterioration and failures that can render them no longer threat representative. Models and simulations often require updates due to intelligence data, operating system, or compiler changes.

The accreditation process establishes sufficient criteria and provides sufficient grounds for use of the threat representation in testing. Threat representation accreditation reflects all the relevant information available from validation testing and provides test organizations adequate information to determine whether or not it is credible and adequate capability for its intended test application. A current, complete validation analysis prior to accreditation for operational testing provides evidence of the threat representation realism to permit the operational analysts to assess the threat representation's contribution to an operational or live fire test event. If the threat representation is sufficient, the OTA (accreditation authority) certifies it for a specific test application.

For programs under DOT&E oversight, the Director, OT&E concurs on the use of any threat surrogate for operational or live-fire testing prior to the initiation of threat accreditation activities. In support of obtaining this concurrence, validation results and the underlying data are provided to DOT&E.

CH 8–3.16 T&E of Defense Business Systems

The majority of programs implementing Defense Business Systems (DBS) pursue commercial off-the-shelf (COTS) product solutions, and many DBS (especially large DBS) are based on well-established commercial Enterprise Resource Planning (ERP) systems. This results in several T&E considerations unique to DBS.

A summary of the T&E planning for developmental and operational test, jointly developed by the program manager, the functional sponsor, and the T&E community are included in acquisition strategies, TEMPs, etc. Early on in requirements development, DBS programs should perform a risk-based assessment to determine the level of testing needed to provide information to the decision-maker and validate requirements. Generally, the risk increases as the amount of modifications to the commercial product increases.

DBS normally do not employ the JCIDS process for development and validation of capability requirements. PMs document requirements in their Problem Statement, defining requirements as business needs supported by measurable business outcomes. The tester must work closely with the system engineer to ensure these business measurements are translated into functional requirements of the software solution.

The strategy for testing DBS considers data collected from both external sources and independent government testing to verify vendor's claims related to a product's functionality, reliability, maintainability, and compatibility.

DBS with Federal financial management capabilities meet auditability and financial compliance requirements as required by current statute and DoD policies. T&E planning includes a comprehensive process of auditability/financial compliance testing, including penetration testing focused on financial fraud/denial of service information.

For more information on Defense Business Systems, refer to DoDI 5000.75.

CH 8–3.17 Software T&E

The DoD acquisition process delivers systems providing secure, resilient capabilities in the expected operational environment. Software is a major driver of the functionality of components of DoD systems. Software T&E, particularly for business and communication systems, is distinct from traditional T&E, predominantly because there is no manufacturing involved. Software is developed and deployed, as opposed to being developed, manufactured, and deployed, in accordance with DoDI 5000.02 (Encl. 3, para 11 – page 61). Software T&E examines system performance from the perspectives of functionality, sustainability, and cybersecurity.

CH 8–3.17.1 Software T&E Overview

In accordance with DoDI 5000.02 (Encl. 5, para 7 – page 73), T&E of software considers the following principles:

- Are the software requirements documented and specified well enough to support T&E? Test planning requires engagement among managers, designers, testers, and users early in the development process, beginning as soon as practical after the Materiel Development Decision (MDD). Bi-directional traceability is established early for individual requirements with the software components implementing them (i.e., which components fulfill each requirement and what requirements do each component contribute to fulfilling). Early bi-directional traceability between components and test cases that test the correctness of their implementation is also needed. The Materiel Developer should work with the software developer to minimize the complexity of the software design and prepare the correct number of test cases for T&E purposes. During testing, performance monitoring relies on operational metrics derived from well-documented software requirements.
- What are the risks? Although software can be relatively inexpensive to change compared to hardware, some risks demand robust software testing and assurance prior to deployment. Mission critical functionality, operational dependability, and cybersecurity are usually high risks for software. All systems capable of sending or receiving digital information are required to conduct some level of cybersecurity testing. Software reliability and security are measured according to the latest available standards.
- Can the software be sustained? Is it reliable and maintainable? We can take advantage of zero-cost manufacturing and transport if we can assure ourselves that new software versions won't destroy previously functioning capabilities. Software developed consistent with good architectural and coding practices is cheaper to maintain and quicker to modify and release to operations, contributing to mission agility. Certain defects in non-critical software functionality that can be fixed later may be acceptable from the perspective of Office of the Secretary of Defense (OSD) oversight during test, provided the software is being managed well enough. Software maintainability is measured to the latest available standards.
- Can we make efficient use of tests and test tools to satisfy certification and other needs (and other standard T&E planning concerns)? For example, an operationally realistic maintenance environment during testing is developed and sustained to enable full capabilities for software patching and upgrades, software modification rollback, and automated regression testing.

CH 8–3.17.2 Software T&E Planning

Software test planning and test design are started in the early stages of functional baseline definition and iteratively refined with T&E execution throughout the phases of development, integration, system qualification, and in-service maintenance, in accordance with DoDI 5000.02 (Encl. 3, para 11 – page 61). PMs involved with software acquisition need to understand at Milestone B how system logs and system status records interface with operational command and control. Automated collection and parsing of performance data are incorporated, as much as possible, into the system design, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(12) – page 68).

Software design and testing is greatly improved through in-depth reviews of selected aspects of the acquisition. These include:

- Architectural Review. Systems engineers and operational maintainers review the information architecture to ensure compliance with established standards.
- Cybersecurity Review. Operational network attackers and defenders engage with system designers in a table-top exercise to articulate expected cyber threats and defenses. For business systems, this includes the threat of financial fraud. The goal of the exercise is to validate and improve the system design for security.
- Development and Maintenance Review. The operational sustainment activity and developing activity jointly discuss and plan the software sustainment environment(s). This environment includes configuration control, defect tracking, and prioritization using the definitions contained in Annex J of IEEE Standard 12207.2, a high-fidelity simulation of the production environment for pre-production test, and automated testing within that environment that meets the statutory and regulatory test automation requirements. This review also includes metrics of reliability, performance efficiency, security, and maintainability.
- User Interface Review. Operational testers assist the Chief Developmental Tester and the developing activity in designing and executing an event that enables the developers to observe operational and administrative users interacting with prototype system interfaces in operationally realistic system use cases.
- Workflow Review. Operational testers and the developing activity participate in a table-top exercise that solicits feedback from operational and administrative users on the planned system workflows.
- Quality Assurance Plan Review. Operational testers, program managers, and other affected staff review the overall quality assurance plan incorporating all reviews, testing, and other quality assurance activities including those described above; ensuring they are incorporated into and are consistent with the development and delivery plans and requirements, and staff and necessary resources are available as needed to ensure completion of all quality assurance activities according to schedule.

All programs on DOT&E oversight require an Initial Operational Test and Evaluation (IOT&E). For software programs not on DOT&E oversight, the OTA determines whether an IOT&E is required. For software, early OT&E events normally support acquisition milestones, which incorporate substantial operational realism, in accordance with DoDI 5000.02 (Encl. 5, para 7 – page 73). Primarily, these events determine a system's potential for operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality before more extensive deployment. IOT&E can also be used to support system certification and training requirements. As feasible, testing is supported by a model (or emulated hardware or virtual machine) of the digital device(s) on which the software runs.

At IOT&E (or at a prior test event), PMs plan to demonstrate within a realistic environment:

- Performance monitoring of operational metrics to manage and operate each system capability (or the whole system, as appropriate).
- Operational suitability, including a demonstrated capability to maintain the software and a measurement of software maintainability.
- Software maintenance sustainment, including patch deployment, software upgrades, and rollbacks. (PMs need to sustain an operationally realistic maintenance test environment in which software patches can be developed and upgrades of all kinds (developed or commercial) can be tested), in accordance with DoDI 5000.02 (Encl. 5, para 7(a)(4) – page 73).
- End-to-end regression testing and defect tracing with such testing automated to the extent feasible in the maintenance test environment.

IOT&E for Incrementally Fielded Software Intensive programs normally consists of a full IOT&E event prior to the Full Deployment Decision (FDD), and are often conducted in a live mission environment so that little or no injection of specific mission threads is possible. Thus, the IOT&E events are guided by an updated assessment of the operational risks in the capabilities and system interactions that have not been successfully evaluated in previous operational testing. Nevertheless, developmental testing strives to investigate as much of the operational envelope as possible, including system response to anomalous inputs (so-called "negative testing").

CH 8–3.17.3 Risk-based Operational T&E of Software

In accordance with DoDI 5000.02 (Encl. 5, para 7(d)(1) – page 73), OT&E for software is guided by the assessment of operational risks of mission failure. A significant operational risk of mission failure is a risk at least moderately likely to occur, and if the risk does occur, then the impact causes a degradation or elimination of one or more mission-critical operational capabilities. The T&E strategy includes an evaluation by the T&E WIPT (or ITT) of the highest risk technologies in system design as well as any areas of excessive complexity in the system software architecture. Programs use standard metrics of the reliability, performance, and security risk of software to assess software risk. Cybersecurity is usually a high risk in software, and it is almost always necessary that a vulnerability and penetration assessment and a cyber-adversary assessment be conducted—the results of which are provided to DOT&E.

DOT&E Memorandum, Guidelines for Operational Test and Evaluation of Information and Business Systems, allows for three levels of software OT&E approval and execution for programs on DOT&E oversight:

- At higher risk, DOT&E approves, observes, and reports on the test.
- At middle risk, DOT&E approves the plan, but does not observe or report.
- At low risk, the OTA can approve the plan, and observe and report on results.

This policy does not have to apply all-or-nothing to the whole plan. Some aspects of OT can be designated as low risk while others have higher risk. Those parts identified as low risk can be managed internally by the OTA. The risk-based policy is the OTA's tool for flexible test design. OTAs can segment tests into risk-appropriate sub-tests.

Refer to DAG, CH 8.3.17.6., Software T&E in an Agile Environment for more information.

At any level of risk, the lead OTA is responsible for observing testing. At the lowest risk level, the lead OTA reviews plans, and observes developmental testing or integrated testing. At the highest risk level, the lead OTA executes a full OT&E in accordance with the DOT&E-approved test plan. For intermediate risks, the lead OTA coordinates with the responsible developmental testing organization to observe and execute integrated developmental testing/operational testing in accordance with a DOT&E-approved test plan. In all cases, the lead OTA informs DOT&E of the outcome of the OT&E. DOT&E then determines the requirement for a formal report.

All systems capable of sending or receiving digital information have to conduct some level of cybersecurity testing. OTAs conduct a risk assessment, identify all threat vectors, and propose an appropriate level of cybersecurity testing to DOT&E. The test plan contains details of how the operational test agency executes the vulnerability and adversarial assessments, including resources, schedule, expected tools, and data for collection. At a minimum, the software is thoroughly analyzed to detect any instances of the Common Vulnerabilities and Exposures (CVE) "Most Dangerous Software Errors." The plan identifies the environment used for both phases of testing and known test limitations due to anticipated deviations from the intended operational environment. The test plan also identifies the specific cyber threat(s) that the adversarial team is meant to portray, the data to be collected during the assessments, and how mission effects are to be determined.

CH 8–3.17.4 Software Support

For software in any system, the evaluation of operational suitability includes a demonstrated capability to use and maintain the software throughout the system's life cycle. In accordance with DoDI 5000.02 (Encl. 5, para 7(a)(4) – page 73), OT&E looks at the program's ability to sustain an operationally realistic maintenance test environment in which software patches and upgrades can be tested. This includes examining:

- Methods available to support software testing and evaluation in unit, integration, and system test phases across the life cycle.
- Data and configuration management methods and tools.
- The extent to which software T&E is embedded with and complementary to software code production as essential activities in actual software component construction (in contrast to T&E that is planned and executed as follow-on actions after software unit completion).
- Formal software T&E when considering selection and integration of new components with existing system elements.
- Formal, standards-based measurement of software maintainability.

CH 8–3.17.5 Software Test Tools & Environment

Test tools include software products that support test activities such as planning and controlling tests, creating test specifications, maintaining requirements, building initial test files and data, executing tests, maintaining configurations necessary to reproduce faults and failures, analyzing/evaluating test results, and maintaining data regarding test results and processes, in accordance with DoDI 5000.02 (Encl. 5, para 7(b) – page 73).

Test tools can provide benefits to the testing program both in the short and long term. A good testing tool potentially:

- Reduces time and effort for repetitive work; a static analysis tool can check coding standards much faster than a manual effort would.
- Provides more predictable and consistent results; eliminates some of the human elements, such as forgetfulness, incorrect assumptions, and mistakes.
- Provides access to and presents accurate test management information. Some test tools can retrieve test results from a database and display them as a chart.
- Ensures reports or findings are assessed objectively; eliminates potential bias.
- Automated testing tools have virtual users that can simulate user actions for many real users, which save the time and expense of using many real users for testing.

However, purchasing a test tool has some potential risks. These include:

- Underestimating the time, cost, and effort when introducing the tool. There could be difficulties in deploying the tool, or there could be resistance from experienced manual testers.
- Expecting more from the tool than it can deliver.
- Underestimating the time and effort needed to derive benefits from the test tool.
- The tool may be complicated, taking time to learn and requiring user training.
- Over-reliance on the tool. For example, tools can't necessarily analyze, suggest improvements, or evaluate future uses.
- Underestimating the effort required to maintain test assets generated by the tool.
- Failure to maintain data and records regarding tool use and results.

The types of tools for testing include tools for:

- Software Source Code Analysis and Measurement
- Unit and Integration Testing
- Data Collection for Performance Testing
- Software Functional and Regression Testing
- Software Load Testing
- Test Management.

The types of tools for related functions include tools for:

- Requirements Management
- Incident Management and Recording
- Configuration Management
- Continuous Integration and Build Management.

CH 8–3.17.6 Software T&E in an Agile Environment

Testing in an agile environment places more T&E focus at the unit level. Compared with non-agile methods, T&E:

- Occurs earlier in the development cycle.
- Occurs in closer cooperation with the developers.
- Occurs more frequently in shorter cycles.

CH 8–3.17.7 Other Software T&E Planning Concerns

Within the DoD acquisition domain, essential considerations for success in testing software include a structural quality and security-focused code audit/analysis as part of the Software Development Life Cycle (SDLC), in accordance with the most current Application Security and Development Security Technical Implementation Guide (STIG) and other relevant guidance documents for Java Run Time Environments and for the .NET Framework.

The following links provide additional information:

- Handbook of Software Reliability Engineering, published by IEEE Computer Society Press and McGraw-Hill Book Company (specifically, CH 13).
- The Consortium for IT Software Quality (CISQ), Specifications for Quality Characteristic Measures.

Medical devices and systems must comply with the SEP, in terms of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104.191) and Risk Management Framework (RMF) information protection procedures and measures. These procedures and measures ensure the software complies with the security standards specified in HIPAA as well as Subtitle D of the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title VIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (P.L. 111.5). Most medical devices require Information Management/Information Technology (IM/IT) testing and validation of information security protocols. Given that requirement, programs start test planning as early as possible. Programs also validate U.S. Food and Drug Administration (FDA) clearance prior to any medical software implementation.

This strategy identifies and describes:

- Required schedule, materiel, and expertise.
- Software evaluation metrics for Resource Management, Technical Requirements, and Product Quality, including Reliability, Security, Performance, and Maintainability.
- Models and simulations supporting software T&E, including accreditation status.

A defined T&E process is consistent with and complements software and system development, maintenance, and system engineering processes, is committed to continuous process improvement, and is aligned to support project phases and reviews, including an organizational and information flow hierarchy.

CH 8–3.18 Network-Centric Operations

Implementation of the DoD's transformation strategy as well as calls for shifting to an Information Age military, results in fewer platform-centric and more net-centric military forces. This requires increased information sharing across networks. The net-centric concept applies to a DoD enterprise-wide information management strategy that includes not only military force operations, but also all defense business processes, such as personnel actions, fuel purchases and delivery, commodity buying, deployment and sustainment activities, and acquisition and development. Key tenets of the strategy include:

- Handling information only once.
- Posting data before processing it.
- Users accessing data when needed.
- Collaborating to make sense of data.
- Diversifying network paths to provide reliable and secure network capabilities.

The shift away from point-to-point system interfaces to net-centric interfaces brings implications for the T&E community. The T&E community's challenge includes representing the integrated architecture in the intended operational environment for test. Furthermore, the shift to net-centric capabilities evolves gradually, no doubt with legacy point-to-point interfaces included in the architectures. PMs, with Program Executive Officer (PEO) support, work with the operating forces to integrate operational testing with training exercises, thereby bringing more resources to bear for the mutual benefit of both communities. It remains imperative that the T&E community engages the user community to assure that test strategies reflect the intended operational and sustainment/support architectures as well as interfaces where they test and evaluate intended capabilities, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(6) – page 67).

CH 8–3.19 Cyber Ranges

This section supports DAG CH 3.7.5., Cybersecurity T&E.

Cyber ranges provide capabilities and environments, which can be integrated at the appropriate classification levels to conduct research, development, experimentation, and testing of military capabilities within a cyberspace environment. They also can support training of military personnel in conducting cyber operations; development of tactics, techniques, and procedures (TTPs); and demonstrating the sustainment of critical missions in cyber-contested environments**.** Use of cyber ranges can provide a more realistic environment while minimizing risk to operational networks, particularly where the employment of cyber effects is impractical or high-risk. Other applications of cyber ranges include:

- An assessment of the scope and duration of advanced cyber effects.
- Component-level system interoperability testing.
- Combinations of developmental, operational, and integrated testing.

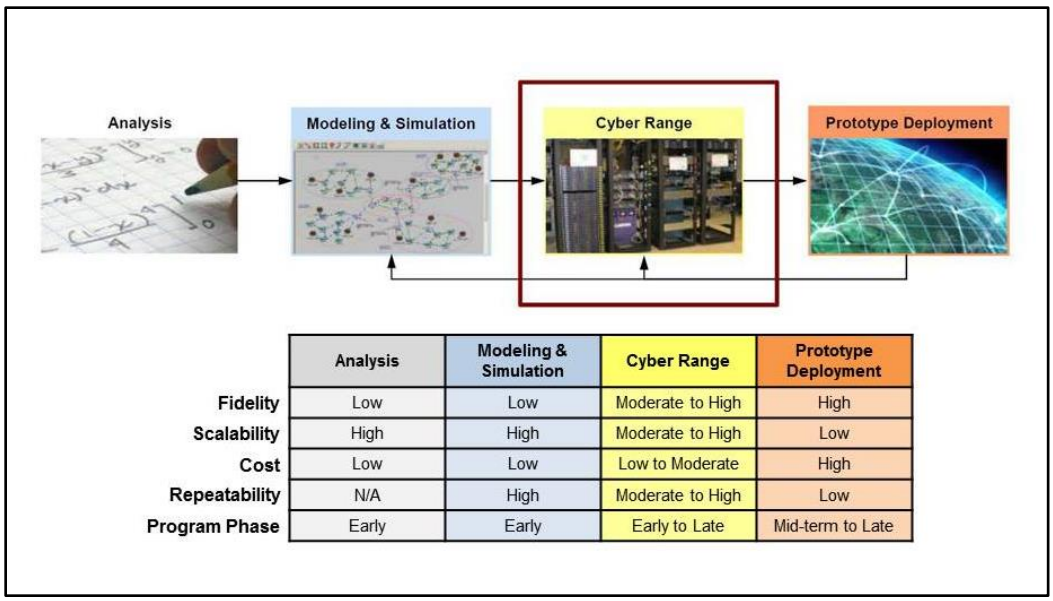
- Assessment and Authorization (Risk Management Framework) processes, in accordance with DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT).
- Immersive training with rapid experience building.

Adequate DT&E, OT&E, and assessments might include testing on cyber ranges due to one or more of the following reasons:

- Testing cannot occur on open operational networks.
- Representation of advanced cyber adversarial TTPs are not suitable for operational networks.
- Scaling requirements (e.g., number of users, hosts, or interconnected systems, amount of network traffic, etc.) cannot be otherwise achieved.
- Operational complexity and associated mission risk are such that the impact to operational networks is avoided.

The program office/Chief Developmental Tester works with the Lead DT&E Organization, cybersecurity dedicated professionals, Operational Test Agencies, DASD(DT&E), and DOT&E to incorporate cyber ranges into the overall test, evaluation, and assessment strategy. (Note: cyber ranges have not been used in lieu of OT&E, and they must be validated and accredited prior to their use for OT&E. In general, the Chief Developmental Tester, Security Control Assessor (SCA), OTA, and PM complete the following actions as early as possible in the acquisition life cycle:

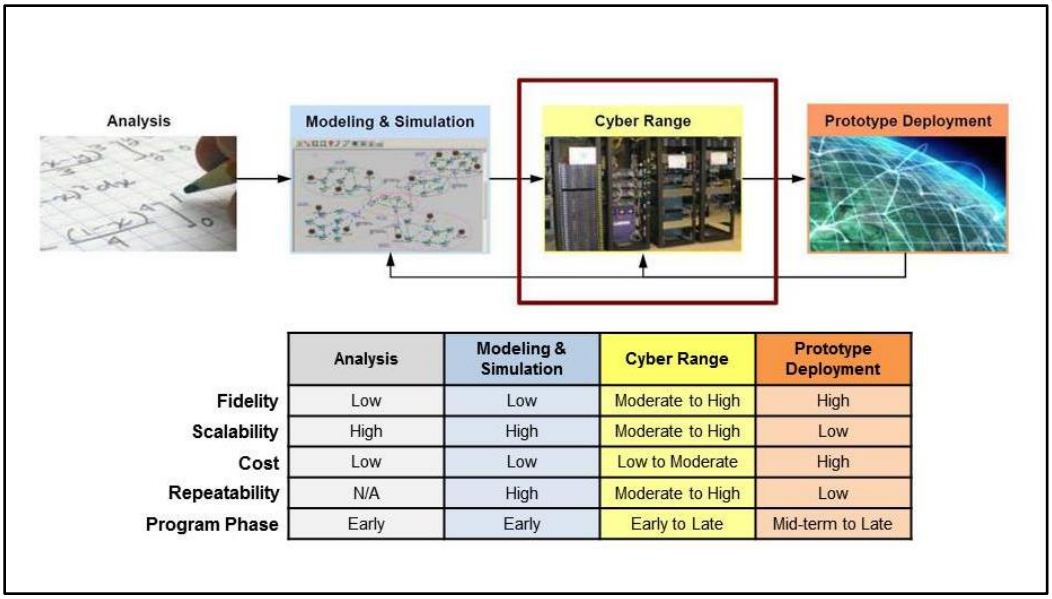
- Identify all testing that will occur on a Cyber Range.
- Identify cyber events for integration with DT&E, OT&E, and assessment activities.
- Support development of linkages between the cyber range and developmental and operational networks.
- Plan for integration of system operators, network defenders, and threat emulations on the cyber range.
- Coordinate with cyber range staffs to ensure they understand the system under test (SUT), operational environment, user space, threat, test objectives, and planned test scenarios.
- Ensure intelligence community support to accurately represent adversarial threats and targets.
- Take measures to verify targets and offensive capabilities emulated on the range are realistic and representative.
- Ensure the entire emulated environment is of adequate fidelity to accomplish test objectives, support technical assessment, and demonstrate impact on operational mission. Emulated environments include:
    - Red – Any capability or environment attributed to adversary forces.
    - Blue – Any capability or environment attributed to own forces.
    - Gray – Cyber environment not owned by any military force, but leveraged by all cyber forces to obfuscate their actions.
- Coordinate with cyber range staffs to investigate any automated data collection capabilities that could support the test.



	Analysis	Modeling & Simulation	Cyber Range	Prototype Deployment
Fidelity	Low	Low	Moderate to High	High
Scalability	High	High	Moderate to High	Low
Cost	Low	Low	Low to Moderate	High
Repeatability	N/A	High	Moderate to High	Low
Program Phase	Early	Early	Early to Late	Mid-term to Late

provides some guidance for choosing a cyber-event environment.

Figure 2: Cyber Event Environment



	Analysis	Modeling & Simulation	Cyber Range	Prototype Deployment
Fidelity	Low	Low	Moderate to High	High
Scalability	High	High	Moderate to High	Low
Cost	Low	Low	Low to Moderate	High
Repeatability	N/A	High	Moderate to High	Low
Program Phase	Early	Early	Early to Late	Mid-term to Late

Table 8: Cyber Ranges provide an overview and contact information for the four DoD cyber ranges.

Table 8: Cyber Ranges

Cyber Ranges				
Range	**Command, Control, Communications, and Computers Assessment Division (C4AD)** Suffolk, VA Contact E-Mail: JS.DSC.J6.MBX.C4AD-operations@mail.mil	**DoD Cybersecurity Range** Quantico, VA Contact E-Mail: IARangeCMT@ITSFAC.com	**Joint Information Operations Range (JIOR)** Norfolk, VA Contact Phone Numbers: (757)836-9787 or (757)836-9848	**National Cyber Range (NCR)** Orlando, FL Contact E-Mail: osd.pentagon.ousd-atl.mbx.trmc@mail.mil
Mission	C4AD conducts assessments of existing and emerging Command, Control, Communications, and Computers (C4) capabilities in a persistent C4 environment to achieve interoperable and integrated solutions that satisfy Joint operational requirements. Replicates Joint Warfighter C4 systems and addresses the interoperability of those systems.	Provides a persistent environment to support test and evaluation, exercise support, training, and education. A simulated representation of the Global Information Grid (DoD Information Network (DoDIN)) Tier 1 environment, complete with network services for realistic system/network evaluation.	Creates a flexible, seamless, and persistent environment (infrastructure) that enables Combatant and Component Commanders to achieve the same level of confidence and expertise in employing information operations (IO) weapons that they have in kinetic weapons.	Provides a high-fidelity, realistic cyber environment to conduct sophisticated cyber training and support cyber testing during all phases of the system life cycle as well as testing of complex system-of-systems. The NCR enables a revolution in national cyber capabilities and accelerates technology transition. Includes agile setup of Multiple Independent Levels of Security (MILS) – sanitized Unclassified, Secret, or SCI environments for cyber training. and Program of Record testing.

Cyber Ranges				
Capabilities	• C4AD can connect to the Joint Information Operations Range (JIOR) or operate in stand-alone mode. • Replicates operational Command and Control (C2) environments with actual hardware and software, enabling assessments of system and system-of-systems interoperability, operational capability, procedural compliance, and technical suitability to confirm readiness for deployment. • C4AD has demonstrated experience combining training exercises and test events to accomplish both test and training, and certification objectives.	• The DoD Cybersecurity Range can operate in stand-alone mode or the Combatant Commanders/Services /Agencies (CC/S/A) with their individual cyber environments, can connect into the range through: ○ The Joint Information Operations Range (JIOR) ○ A Virtual Private Network (VPN) over the Internet and Defense Research and Engineering Network (DREN). • Persistent environment focused on cybersecurity and computer network defense. • Representation of the DoD Information Network (DoDIN) Tier 1 Environment, complete with network services, for realistic system/network evaluation. • Provides generic DoD Tier II and Tier III capabilities. • Services include traffic generation, configurable user emulation. Malware, spyware, and BOTnets can be emulated and employed in the environment to stimulate training.	• Closed, multi-level security (Top Secret/ Sensitive Compartmented Information (TS/SCI) environment built to conduct cyber and other non-kinetic activities. • Distributed network with service nodes at approximately 68 locations. • Forms a realistic and relevant live fire cyberspace environment supporting Combat Commands, Service, Agency, and test community training, testing, and experimentation across the IO and Cyberspace mission areas. • Can provide secure connectivity and transport for Coalition Partners. • Multiple simultaneous events at multiple levels of security. • Meets Capstone Concept for Joint Operations intent and provides a critical Joint Force cyberspace training and testing environment. It is the only “live fire” range supporting cyberspace and IO-related objectives in the Joint Training Enterprise.	• NCR can connect to the JIOR, JMETC Multiple Independent Levels of Security (MILS) Network (JMN), or operate in stand-alone mode. • Specialized software facilitates rapid network design, reconfiguration, and sanitization, as well as network scaling. • Security architecture that enables a common infrastructure to be partitioned into MILS and leverage real malware. • End-to-end toolkit that automates the lengthy process of creating high-fidelity test environments. • Unique combination of subject matter expertise in cyber domain, cyber testing, cyber range management, and cyber testing tools.

Error! Reference source not found. provides a list of additional cyber resources and facilities accessible to DoD organizations.

Table 9: Other Cyber Resources & Facilities

Resource/Facility	Mission	Capabilities

Joint Mission Test Environment Test Capability (JMETC)
 	
Test Resource Management Center (TRMC)
 	
Alexandria, VA
 	
Contact Email:
 	
osd.pentagon.ousd-atl.mbx.trmc@mail.mil
 	
Contact Phone Number(s):
 	
571-372-2697
 	
571-372-2701
 	
571-372-2702
	JMETC provides the persistent, robust infrastructure (network integration software, tools, re-use repository) and technical expertise to integrate Live, Virtual, and Constructive systems for test and evaluation in Joint System-of-Systems and Cyber environments.	• JMETC SECRET Network (JSN) provides a distributed network infrastructure with 76 geographically separated nodes connecting live systems, Hardware-in-the-Loop (HWIL), Installed Systems Test Facilities (ISTF), and Virtual/Constructive simulations representing the system under test on range and laboratory facilities.
		• JMETC Multiple Independent Levels of Security (MILS) Network (JMN) provides closed connectivity between and among Cyber Ranges and Live, Virtual, and Constructive (LVC) test assets at multiple levels of classification Secret, Top Secret, Top Secret/Sensitive Compartmented Information, Special Access Program/Special Access Required (S, TS, TS/SCI, SAP/SAR). JMN provides the ability to peer with JIOR.
		• JMETC also maintains and provides access to Regional Service Delivery Points (RSDP), which provides the ability to create virtualized cyber environments for cybersecurity testing. RSDPs are:
		  ○ Extensible to cyber ranges to create more complex, higher scale environments.
		  ○ Provide enterprise computer storage as well as hosting common tools and services for the Cyber T&E, training, and experimentation communities.
		  ○ Geographically distributed to minimize latency and accessed through the JMN. There are currently two deployed RSDPs, with others planned for deployment.
		• Capabilities typically provided at no additional cost to the customer.

CH 8–3.20 Rapid Fielding Testing

One of DoD's highest priorities is to provide warfighters involved in conflict or preparing for imminent contingency operations with the capabilities urgently needed to overcome unforeseen threats, achieve mission success, and reduce risk of casualties. Joint Urgent Operational Needs (JUONs), Joint Emergent Operational Needs (JEONs) and related rapid acquisition activities are intended to support these efforts. In accordance with DoDI 5000.02 (Encl. 4, para 5(e) – page 68), required testing to verify safety, capabilities, and limitations is performed consistent with the urgency of fielding the capability. In collaboration with the supporting operational test organization, the PM for a rapid acquisition activity develops a highly tailored and abbreviated TEMP, which is consistent with the Acquisition Strategy (AS), in accordance with DoDI 5000.02 (Encl. 5, para 5(c)(1) – page 71). The TEMP describes a performance assessment plan that includes a program and test schedule, metrics, test methodologies, and test assets required. While the operational testing described is tailored and abbreviated, as much as possible, it follows the basic tenets of operational testing described in DAG CH 8.3.2.1., Evaluation of Operational Test Adequacy**.** If the program has been placed on DOT&E oversight, the PM has the TEMP approved by the DOT&E. The MDA, in consultation with the supporting operational test organization, and with the approval of DOT&E for programs on DOT&E oversight, determines the requirement for post-fielding assessments, whether the urgent need solution has been adequately reviewed, performs satisfactorily, is supportable, and is ready for production and deployment. DOT&E reports the results of required testing to the Secretary of Defense and provides copies to Congress and the MDA.

CH 8–3.21 T&E of Unmanned & Autonomous Systems

Test and evaluation programs involving Unmanned and Autonomous Systems (UAASs), as either a stand-alone system or as part of a system-of-systems, consider the increased technical complexity for testing, as well as challenges for range safety approval. The TEMP addresses the approach and T&E resources required to verify the performance of autonomous and semi-autonomous systems in making decisions for achieving the objectives of unmanned platforms such as aircraft, ground vehicles, or sea vehicles. The TEMP complies with DoDD 3000.09, Autonomy in Weapon Systems, to assess the risk of failures that could lead to unintended engagements or to loss of control of the system. Added to this complexity are the cybersecurity and interoperability requirements with companion platforms.

Test and evaluation of autonomous decision-making processes involves a new form of testing that allows for not knowing all input conditions being used by an algorithm, which in and of itself may be constantly changing its form. All that a tester may know for certain is the "statement of the success criteria" that the autonomous decision-making process is trying to satisfy. Significantly, this suggests that not only the tester tests the ability of the decision-making process to deliver a solution that enables successful mission completion; the tester may also now be testing the adequacy of the statement of the success criteria itself. While T&E of platforms and automated software are well-established disciplines, the emerging challenge confronting T&E involves how to adequately test a system's decision-making processes in which all inputs cannot be predicted, the algorithm may be changing, and repeatability is unlikely. Discovery of functionality, design, or integration issues after a system has been approved to enter production, or even worse, IOT&E, can adversely affect acquisition program cost and schedule; and most such issues result from lack of consideration of aspects on how a system is used or the environment in which it is intended to operate.

CH 8–3.22 Competitive Prototyping

Competitive prototyping is one of the areas the T&E WIPT (Chief Developmental Tester, Lead DT&E Organization, empowered representatives of test data producers and consumers) considers during development of the Milestone A TEMP. Competitive prototypes are part of the TMRR Phase unless specifically waived by the MDA at or prior to Milestone A.

A competitive prototype, or if this is not feasible, a single prototype or prototyping of critical subsystems prior to Milestone B is statutorily required to be part of the Acquisition Strategy for MDAPs, and is a regulatory requirement for all other programs, in accordance with P.L. 111-23, SEC. 203, Weapon Systems Acquisition Reform Act of 2009.

CH 8–3.23 EOD Validation & Verification Testing

DoDD 5160.62, Single Manager Responsibility for Military Explosive Ordnance Disposal Technology and Training (EODT&T), ensures that Military Department programs for the acquisition of explosive ordnance materiel and activities (including applicable weapon delivery systems) provide technical data and make available hardware for Explosive Ordnance Disposal (EOD) validation and verification testing, and recommend any unique tools necessary for EOD procedures.

This Directive requires:

- Testing and transportation of developmental explosive ordnance, including foreign ordnance being evaluated for possible U.S. acquisition, and does not begin until sufficient data on its hazards and functioning are available for EOD response to incidents or accidents during transportation and testing.
- EOD procedures, tools, and equipment to be developed, tested, jointly verified, and fielded before fielding of new explosive ordnance.
- Secretaries of the Military Departments to establish management controls to ensure that all programs for acquisition of explosive ordnance and applicable weapon delivery systems provide for the development of EOD technical source data in accordance with the specifications of the Single Manager for EODT&T, the availability of hardware for Joint EOD validation and verification testing, and the recommendation of tools necessary for EOD render-safe and disposal operations. All developers of explosive ordnance and applicable weapons delivery systems (except nuclear systems) provide sufficient quantities of inert and live explosive ordnance items for Joint validation and verification of EOD procedures and EOD training.

MIL-STD-882E (Para 4.3.2. – page 10), DoD Standard Practice for System Safety, identifies the DoD approach for identifying hazards and assessing and mitigating associated risks encountered in the development, test, production, use, and disposal of defense systems.

MIL-STD-882E (Task 101, para 101.2.5. – page 22) recommends reporting on the assessment and status of hazards at system, subsystem, and component technical reviews, such as the System Requirements Review (SRR), Preliminary Design Review (PDR), Critical Design Review (CDR), Test Readiness Review (TRR), and Production Readiness Review (PRR). The Standard identifies the requirements for certifications, independent review board evaluations, and special testing (e.g., insensitive munitions tests, Hazards of Electromagnetic Radiation to Ordnance (HERO), Electrostatic Discharge (ESD), and render-safe/emergency disposal procedures).

In accordance withMIL-STD-882E (Task 303 – page 82), T&E planning includes the following:

- Participation in the preparation and updating of the TEMP, including hazard considerations and identification of when hazard analyses, risk assessments, and risk acceptances shall be completed in order to support T&E schedules.
- Participation in the development of test plans and procedures, including hazard considerations that support:
    - Identification of mitigation measures to be verified and validated during a given test event with recommended evaluation criteria.
    - Identification of known system hazards present in a given test event, recommended test-unique mitigations, and test event risks.
    - Preparation of the Safety Release.
    - Analysis of hazards associated with test equipment and procedures.
    - Government completion of applicable environmental analysis and documentation pursuant to DoD Service-specific National Environmental Policy Act (NEPA) and Executive Order (EO) 12114 requirements in test and evaluation planning schedules.

    - Documentation of procedures for advising operators, maintainers, and test organizations involved in the test event of known hazards, their associated risks, test-unique mitigation measures, and risk acceptance status.
- Conduct of post-test event actions such as:
    - Analyze test results to assess effectiveness of mitigation measures as tested.
    - Analyze test results to identify and assess new system hazards and to potentially update risk assessments for known hazards. MIL-STD-882E provides more information.
    - Analyze incident, discrepancy, and mishap reports generated during test events for information on hazards and mitigation measures. Ensure mitigation measures are incorporated in future test plans as appropriate.
    - Document new or updated system-related hazard information in the Hazard Tracking System (HTS), as appropriate.

CH 8–3.24 Safety Reviews

DoD is committed to protecting personnel from accidental death, injury, or occupational illness and safeguarding defense systems, infrastructure, and property from accidental destruction or damage while executing its mission requirements of national defense.

Integral to these efforts is the use of a system safety approach to identify hazards and manage the associated risks. A key DoD objective is to expand the use of this system safety methodology to integrate risk management into the overall Systems Engineering (SE) process rather than addressing hazards as operational considerations.

MIL-STD-882E (Para 1.1.1. – page 1) identifies the DoD SE approach to eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated. DoDI 5000.02 (Encl. 3, para 16(b) – page 63) identifies risk acceptance authorities for Environment, Safety and Occupational Health (ESOH). MIL-STD-882E covers hazards as they apply to systems/products/equipment/infrastructure (including both hardware and software) throughout design, development, test, production, use, and disposal.

The Chief Developmental Tester coordinates with the Program Lead System Engineer to identify the required safety reviews in support of T&E efforts and provide the required information. In-addition, the Chief Developmental Tester needs to coordinate with the program engineer for development and safety releases in support of T&E events in accordance with Component direction and guidance.

For more information, see MIL-STD 882E, DoD Standard Practice for System Safety.

CH 8–3.25 Medical Materiel T&E

The acquisition and management of medical materiel presents distinct challenges to the design and execution of an effective test and evaluation (T&E) program within the DoD acquisition framework.

Medical materiel acquisition is subject to the same laws and regulations as those governing other defense systems and has similar requirements for T&E. Frequently, the products considered for acquisition are commercial off-the-shelf (COTS), government off-the-shelf (GOTS), non-developmental items (NDI), and similar items adapted or repackaged for military use. For pharmaceuticals, medical devices, and monitoring systems, the minimum standard for use is certification or approval by federal regulating agencies, typically the U.S. Food and Drug Administration (FDA) or the Environmental Protection Agency (EPA). Appropriately constructed requirements documentation includes such certification or approval as a specified system key performance parameter (KPP). Planning for T&E of medical materiel systems begins with the development of user needs and continues throughout the acquisition process. FDA approval or Environmental Protection Agency (EPA) certification of a product, and the data provided from associated testing and clinical trials may provide a significant body of information useful to reduce the scope and cost of testing within DoD acquisition programs.

Additional considerations for medical systems may include requirements related to compliance with the Health Insurance Portability and Accountability Act (HIPAA), human subject research protections, human factors concerns, environmental testing, air-worthiness certifications (fixed and rotary wing) for systems employed on air evacuation platforms, and cybersecurity. Medical systems and devices that capture, store, process, or transmit data over information networks are also subject to the extensive requirements related to cybersecurity, as outlined in DoDI 8500.01 (Encl. 3, para 9(a)(2)(b) – page 39), Cybersecurity.

Use of the T&E WIPT structure is an effective mechanism to coordinate and organize the various entities for execution of the T&E program. Coordination of these activities across the Services in T&E of medical materiel is encouraged; consistent with DoDI 6430.02 (Encl. 4, para 6(d)(6) – page 11), Defense Medical Materiel Program, to promote uniformity, efficiency, and Joint interoperability in acquisition and life-cycle management of medical materiel required for military healthcare delivery in both military treatment facilities and in support of operations.

Refer to the Defense Health Agency, Defense Medical Materiel Standardization Program for additional information.

CH 8–3.26 CBRN T&E

In accordance with DoDI 3150.09 (Encl. 2, para 2(h)(i)(J) – page 10), the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (DASD(NCB)) shall:

- Oversee Chemical, Biological, Radiological, and Nuclear (CBRN) Defense RDT&E.
- Establish CBRN Defense T&E standards in support of CBRN survivability in conjunction with the DASD(DT&E).
- Lead the process to develop Chemical, Biological, Radiological (CBR) contamination survivability test methodologies and standards through the Chemical Biological Defense Program (CBDP).
- Assess the T&E infrastructure and identify essential requirements to support DoD CBRN Survivability Policy initiatives in conjunction with the DASD(DT&E).

CBRN defense consists of several categories. Within the context of CBRN Defense T&E, CBRN survivability is the principal area and is explained in more detail in the following paragraphs.

In accordance with DoDI 3150.09 (Encl. 2, para 5 – page 12), the DASD(DT&E):

- Monitors DoD CBRN survivability policy for impact on current and future T&E policy and guidance, and T&E workforce training and education.
- Ensures that CBRN survivability is assessed for CBRN Medical Countermeasure Systems (MCS) on the USD(AT&L) MDAP, MAIS, and AT&L Special Interest lists.
- Helps the DASD(NCB) develop and review test protocols in support of CBRN survivability requirements.
- Provides representation to the CBRN Survivability Oversight Group (CSOG) and supporting working groups.

Materiel developers work with the operational test agencies, the DASD(DT&E), Office of the CBDP T&E Executive, Defense Threat Reduction Agency (DTRA), and the Military Services to develop strategies and TEMPs that realistically assess the CBRN survivability capabilities and requirements validated in the ICD, CDD, and CPD. Materiel developers will provide all T&E data to the DASD(DT&E) and DOT&E for programs on OSD T&E oversight. Additionally, the Military Departments will ensure that the TEMP describes how the T&E strategy will meet validated CBRN survivability requirements stated in the CDD and CDP for all CBRN MCS, in accordance with DoDI 3150.09 (Encl. 3, para 8(a) & (b) – page 24).

CH 8–3.26.1 CBRN Survivability

DoDI 3150.09 provides policy, assigns responsibilities, and establishes procedures for the execution of DoD Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy. It establishes how to identify mission-critical systems and specifies the subsets that must survive and operate in CBR environments, nuclear environments, or combined CBRN environments.

CBRN survivability is divided into two categories: CBR survivability, which is concerned with CBR contamination, including fallout and nuclear survivability, which covers initial nuclear weapons effects, including blast, electromagnetic pulse (EMP), and other initial radiation and shockwave effects. CBRN survivability is defined as:

> The capability of a system to avoid, withstand, or operate during and/or after exposure to a CBR environment (and relevant decontamination) or a nuclear environment, without losing the ability to accomplish the assigned mission.

Mission-critical systems are the primary focus of CBRN survivability. In accordance with DoDI 3150.09 (Glossary – page 37), a mission-critical system is a system whose operational effectiveness and operational suitability are essential to successful mission completion or to aggregate residual combat capability. If the system fails, the mission likely will not be completed. Such a system can be an auxiliary or supporting system, as well as a primary mission system. A CBRN mission-critical system is a system that is required to be employable and survivable in a CBR or nuclear environment. In accordance with DoDI 3150.09 (Para 3(b) – page 2), all ACAT I programs expected to operate in CBR or nuclear environments are designated as CBRN mission-critical systems. DoD Components are responsible for identifying mission-critical systems and specifying which must survive in CBR, Nuclear, or combined CBRN environments.

DoDI 3150.09 (Para 3c – page 2) directs that CBRN mission-critical systems must be survivable in accordance with the CBRN survivability requirements identified in their requirements documents (e.g., initial capabilities document (ICD), capability development document (CDD), capability production document (CPD)). All CBRN mission-critical systems under development, as a part of a DoD Acquisition System, are required to address CBRN survivability at each milestone, in accordance with DoDI 3150.09 (Para 3(c)(2) – page 2).

A subset of CBRN survivability involves the CBD program (CBDP). The CBDP falls under the auspices of the Joint Program Executive Office for Chemical and Biological Defense (JPEO CBD), which is responsible for providing research, development, fielding, and life-cycle support of CBRN defense equipment, medical countermeasures, and installation and force protection integration. DoDD 5160.05E (Para 7 – page 8) designates and defines the role of the Secretary of the Army as the DoD Executive Agent for CBD programs. As such, the Secretary of the Army is responsible for designating a CBD program T&E Executive, which for CBD programs is the Deputy Under Secretary of the Army for Test and Evaluation (DUSA-TE). The DUSA-TE serves as the T&E Executive for CBRN Defense. As such, the DUSA-TE Office provides CBRN Defense and CBDP T&E Enterprise oversight and coordinates all CBRN Defense T&E issues with the Joint Staff and OSD—specifically, the USD(AT&L), the DOT&E, and the DASD(DT&E).

For additional information and guidance regarding CBRN survivability, contact the JPEO CBD.

CH 8–3.26.2 CBRN Defense T&E

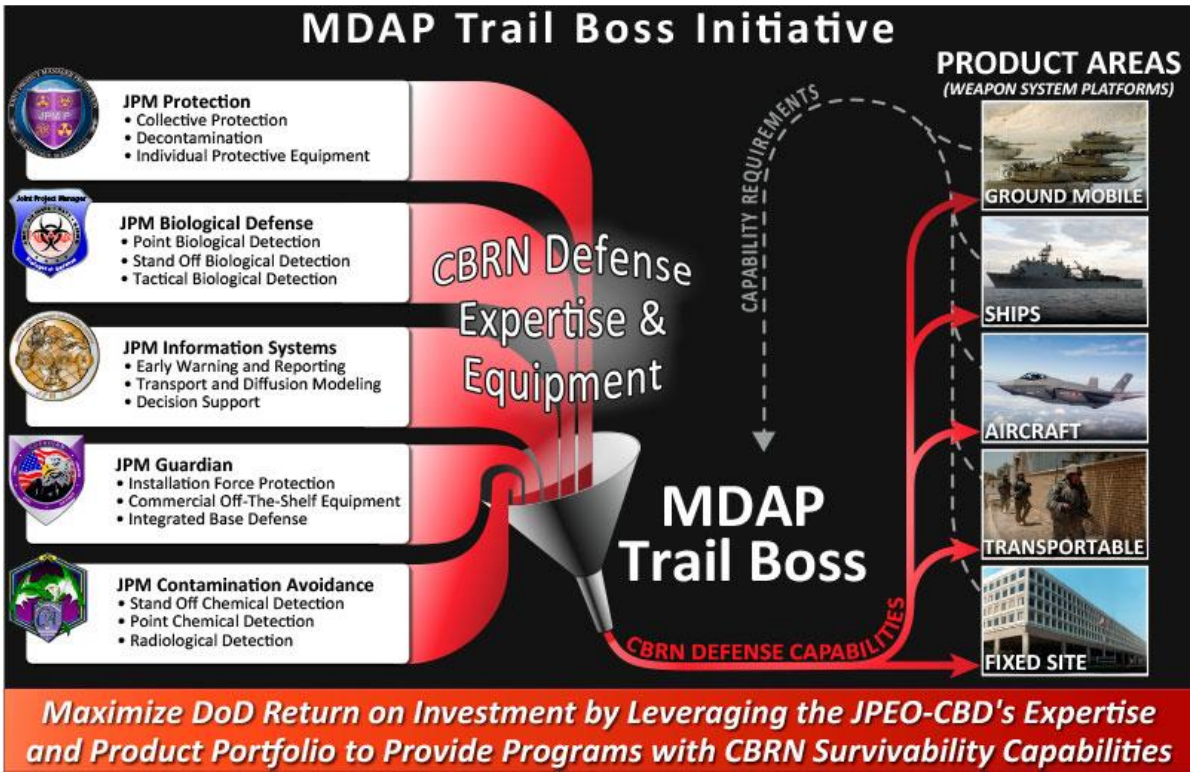
A Chemical, Biological, Radiological, and Nuclear (CBRN) mission-critical system T&E program can involve exposure of the system-under-test (SUT) to chemical and biological warfare agents, toxic industrial chemicals (TICs), toxic industrial materials (TIMs, including radionuclides), and nuclear effects such as radiation, thermal, EMP, shock, etc. Test and evaluation of such systems for vulnerabilities to any of these environments likely entails the use of multiple and geographically dispersed test facilities and associated logistics, stringent safety and security considerations, and risk of destruction of the SUT. These considerations are taken into account when planning and executing a T&E program involving a

mission-critical system. It is also necessary to design a T&E program that leverages data from multiple test approaches, including system or component testing in chemical or biological safety chambers, full-system open air testing with simulants that represent the threat, or with stimulants that trigger end-to-end operational scenarios, and modeling and simulation.

Where CBD programs are concerned, the DUSA-TE employs the T&E Capabilities and Methodologies Integrated Process Team, or TECMIPT (requires registration), to oversee and manage their T&E programs. Through its Commodity Area Process Action Teams (CAPAT), the TECMIPT is responsible for identifying CBRN T&E infrastructure gaps, and developing and reviewing CBRN T&E standards.

JPEO-CBD has established a team of CBRN survivability subject matter experts to assist Service Acquisition Programs designated as CBRN MCS. These CBRN experts assist with the integration of CBD program systems and equipment into weapon's systems. The CBRN Survivability Trail Boss initiative offers weapon system program offices a single point of contact to help facilitate the research, development, T&E, procurement, delivery, and life cycle sustainment of CBRN defense materiel solutions that meet the program's documented requirements.

Figure 3: CBRN Trail Boss Overview



The MDAP Trail Boss initiative supports all ACAT level programs with CBRN survivability requirements. A program office should engage the Trail Boss team early in the requirements development process to leverage their expertise relative to trade space and test capabilities available to measure thresholds and objective CBRN survivability requirements.

For additional information and guidance regarding CBRN survivability, contact the JPEO CBD.

CH 8–3.27 Interoperability Testing of Geospatial Intelligence Systems

Geospatial Intelligence (GEOINT) is a specialized discipline within the defense and intelligence communities. GEOINT is made up of three key elements: geospatial information, imagery, and imagery

intelligence. It is defined in 10 USC 467 as “the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth.”

Due to the proliferation of GEOINT across DoD, compliance with GEOINT interoperability criteria is critical for systems that use, produce, or enable GEOINT. To assure systems collect and/or interact with GEOINT in compliance with mandated standards, the Director, National Geospatial-Intelligence Agency (NGA) is implementing a new process—the GEOINT Functional Manager Standards Assessment (GFMSA) (requires DoD CAC and Intelink Account). The GFMSA serves as recognition that a component of Information Technology (IT) or National Security System (NSS) has been tested and/or evaluated in a credible manner and found to meet the standards conformance and interoperability criteria set by the National System for Geospatial Intelligence (NSG) community. GFMSA is an authoritative means to confirm that interoperable GEOINT capabilities are delivered. Successful completion of the GFMSA T&E process optimizes potential for a system to meet its GEOINT-related operational performance objectives.

GFMSA fulfills the NGA responsibilities identified in DoDI 8330.01 (Encl. 2, para 12(a) – page 17), prescribing, mandating, and enforcing standards and architectures related to GEOINT. NGA, in coordination with the Joint Interoperability Test Command (JITC), the Responsible Test Organizations (RTOs), the Operational Test Agencies (OTAs), and the appropriate intelligence functional managers, develops interoperability T&E criteria, measures, and requirements related to GEOINT. GFMSA Qualifications infuse GEOINT awareness into the generalized net-centric data requirement. Each GFMSA Qualification has a set of GEOINT-aware ‘Criteria’ for measuring qualification success.

Generally, the GFMSA process consists of five basic steps, noting that the steps can be a repetitive/regressive process as conditions change. The steps, as depicted in, are:

Step 1. Identify mission capability requirements and associated MOE and MOP.

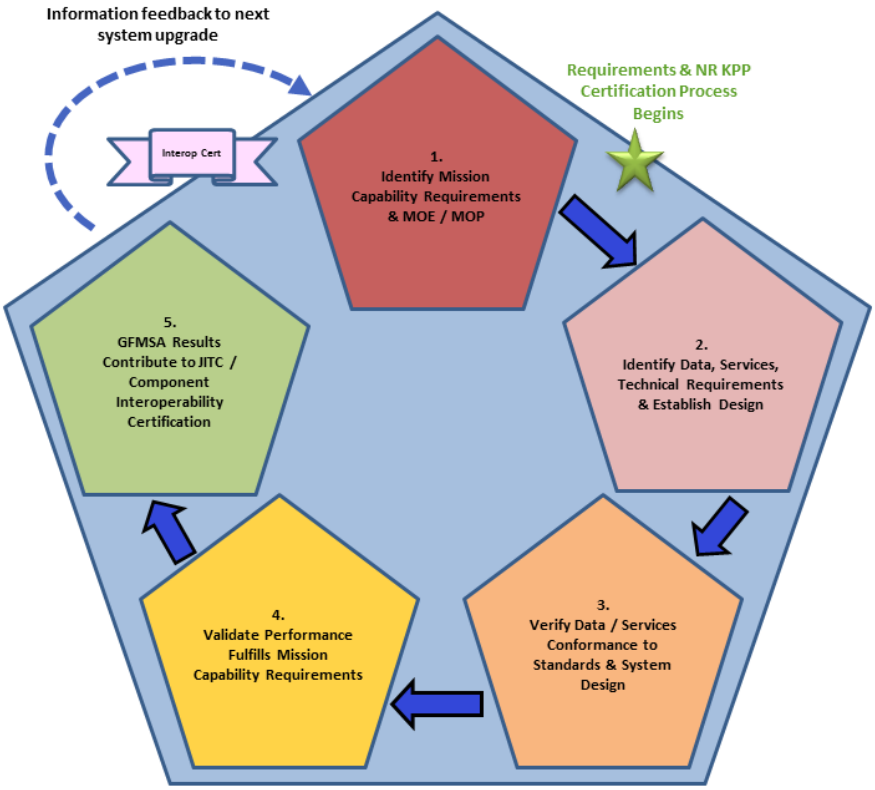
Step 2. Identify data, service, and technical requirements; and establish system and data content design in conformance with applicable GEOINT standards.

Step 3. Verify through T&E that data and services conform to both the GEOINT standards and the system design.

Step 4. Validate through T&E that the performance of the conforming design, data, and services fulfills the mission capability requirements established in step 1.

Step 5. GFMSA test results contribute to an interoperability certification determination. Submit test reports, certifications, and statuses substantiating GFMSA qualification to the Design for Manufacturability (DFM) for Architecture and Standards.

Figure 4: GEOINT Functional Manager Standards Assessment Qualification Cycle



The GFMSA initiative is focused on ensuring consistent conformance to GEOINT standards by systems using, producing, or enabling GEOINT. Conformance to adopted GEOINT standards is critical to the ability of the NSG enterprise to efficiently collect, store, discover, retrieve, and utilize GEOINT data, products, and services in an interoperable manner.

Integrating GFMSA qualification objectives into TEMPs permits DT&E and OT&E testing and test results to support GEOINT-aware Joint interoperability test certification and eliminate test duplication. T&E events used to substantiate GFMSA qualification often span DT&E, OT&E, Interoperability, and other test activities, relying on multiple test events conducted by various test organizations. While conformance with applicable GEOINT standards is an essential step toward GFMSA qualification, the amount and type of testing varies based on characteristics of the component/system being evaluated. Developmental testing performed under government supervision that generates reliable and valid data can be used to determine technical capabilities and standards conformance status, and may supplement operational data for a GEOINT-aware interoperability evaluation. Each potential data collection opportunity is used in the overall T&E process to get the best GEOINT-aware, performance-based picture of the component/system in the most efficient manner possible to substantiate GFMSA qualification.

Refer to the GFMSA Resource Site (requires DoD CAC and Intellink Account) for more information and references.

NOTE: While this section discusses Geospatial Intelligence specifically, there are other intelligence areas that should considered, if relevant.

CH 8–3.28 Testing in a Joint Environment

The phrase “testing in a Joint environment” originated in the U.S. Department of Defense final report, Testing in a Joint Environment Roadmap, Strategic Planning Guidance, Fiscal Years 2006-2011, November 12, 2004. It refers to testing military systems as participating elements in overarching Joint SoS. This testing in a joint operational environment initiative supports the department’s long-term strategy to test as it fights. Joint operations have become the mainstay of warfighting. Force transformation requires the T&E community to place a greater emphasis on testing Joint warfighting capabilities developed in response to the JCIDS process. Future T&E must ensure combatant commanders can rely on equipment to operate together effectively without introducing problems to warfighters. For a detailed discussion of changes needed to bring about this vision of T&E, see the final report cited above.

The Joint Mission Environment (JME) (Section 1.4) is defined as, "the operational context in which the capability being developed must perform." It describes the expected operating environment of the system (or system-of-systems) under test, and includes all of the elements influencing the required performance the new “capability” demonstrates. These include the particular mission requirements in which the system is being employed; physical factors such as the blue and opposing force structures; geographic and demographic aspects of the Joint operating area, etc.; as well as the interactions between these elements.

To be successful, testing in the JME cannot be a new step added at the end of operational T&E, nor can it replace current DT or OT. It does, however, represent a departure from the way DoD acquisition professionals plan and execute systems engineering, DT&E, and OT&E—indeed, the entire acquisition process. Testing in a JME involves the appropriate combination of representative systems, forces, threats, and environmental conditions to support evaluations. These representations can be LVC, or distributed combinations thereof.

Testing in a JME applies throughout the life cycle of the system. Identification of a Joint issue/problem early in a system's life (including as early as the conceptual phase) reduces costs and issues. In accordance with DoDI 5000.02 (Encl. 5, para 5(d)(4) – page 71), this applies to evaluating system performance, or how well the system does what it is designed to do, as well as the system’s contribution to the Joint mission, or how DoD employs the system to achieve the mission. A system’s interaction with the JME is evaluated along an evaluation continuum using constructive and virtual representations and live systems in various combinations.

The JME and associated Joint capability requirements are defined in the ICD, CDD, and the CPD. The evaluation plans for assessing these requirements are articulated in the SEP and the TEMP at Milestone A. At the pre-EMD Review, evaluation plans for assessing these requirements are articulated in the pre-EMD draft documents (SEP, TEMP, and ISP). At Milestones B and C, they are articulated in the SEP, TEMP, and ISP. For each case, the selection of LVC systems used to recreate the JME to support testing depends on the purpose of the assessment and on the interactions the SUT has with other elements in the JME.

SoS testing can result in unexpected interactions and unintended consequences. T&E of SoS not only assesses performance to desired capability objectives, but also characterizes the additional capabilities or limitations due to unexpected interactions. The SoS concept includes the system in the broadest sense, from mission planning to sustainment. SoS is a new and evolving area for development, acquisition, and T&E.

This section also briefly addresses some additional areas as outlined in the “Testing in a Joint Environment Methods and Processes (M&P) Implementation Plan,” originally produced by the M&P Working Group that was formed during the summer of 2004 to address testing in a Joint environment. The following are areas of concern:

- Description of Joint Mission Environments
- How to use the Joint Mission Environment

- Testing in a Joint Mission Environment Program Management Office Support
- Important Acquisition Program Responsibilities.

Refer to the Systems Engineering Guide for Systems-of-Systems for more information on testing in a Joint environment.

CH 8–3.28.1 Description of Joint Mission Environment

The JCIDS process creates requirements for effects and capabilities at the Joint mission level. This means JCIDS identifies desired mission-level effects that are shortfalls. Shortfalls are addressed by materiel and non-materiel solutions. Materiel or possible system (for a new/modified system or SoS) KPPs are then proposed to provide the desired mission level effect(s). Because of this, systems development should not begin and testing cannot occur without definition(s) of the JME and a defined Joint mission associated with a shortfall to be addressed by a system or systems.

With respect to obtaining information for selected Joint missions, users of the Joint environment can start with the universal Joint planning process to break down missions, but it is a process that starts at the Universal Joint Task List (UJTL) level and extends down to the Combatant Command (COCOM) level to plan Joint task force operations and/or training events. However, this level of "fidelity" may not be available at the JCIDS ICD/CDD/CPD level because it is mission-specific at the COCOM or Joint Task Force level.

The Joint mission descriptions set the stage for evaluation of a system(s) within a Joint mission area and provide testers what they need to plan the test. There are essential elements of the Joint mission description necessary to plan, execute, and analyze assessments and T&E throughout a system's acquisition process.

Additionally, users of the Joint environment determine and obtain representations for the threat, threat composition and disposition, and threat scheme of maneuver appropriate for the selected Joint mission/task. The currently approved "Guidance for the Development of the Force (GDF)" scenarios and/or the maturing "Defense Planning Scenarios" provide the source of this information. Coordination with the Service intelligence organizations and the Defense Intelligence Agency (DIA) is critical. The threat should be system-specific (specific to the platform under examination) and also mission-specific (specific to the Joint mission examined). The next step (after identification of the threat scenarios) is to determine what is used to represent the threat, which can be an LVC representation.

Different Services are referred to depending on the type of model needed for test, as the Services have generally focused their modeling efforts based on their usual area of operations. DoD M&S responsibilities are outlined in DoDD 5000.59, DoD Modeling and Simulation (M&S) Management. Additionally, the Modeling and Simulation Coordination Office (MSCO) defines the responsibilities of M&S Executive Agents. There should also be a standard set of environment/background models established for the JME.

CH 8–3.28.2 How to Use the Joint Mission Environment

Systems engineering and testing require insertion of concepts and systems into the JME as a standard part of the acquisition process.

The ultimate goal for systems engineering and testing in a Joint environment is the ability to insert any system into the applicable JME at any time during the life of a system. Two basic items are examined through insertion into the JME. The first item is to ensure the systems to be acquired are interoperable with other systems. This includes not only how they interact and communicate as expected and required, but also understanding SoS dependencies. The second item goes beyond the system interaction and communications to examine what value the systems add to Joint military capabilities. In other words, the second item is to assess the contribution of the system to the mission success.

Interoperability and contribution are examined each time a system is inserted into the JME, including times when substantive changes or upgrades are made to an individual system. Users can determine which Joint mission/task(s) to test for a system with a role in multiple missions.

Selection of the most stressing mission(s) and/or the mission(s) with the most interactions appears to be the most defensible approach. Test authorities must ensure that if another required mission involves a system interaction not included in the "most stressing" mission, the interaction is tested separately. Examining different Joint missions as the system progresses through the acquisition process is also a good approach, especially if there appear to be multiple stressing missions. Another option is to consult with the intended Joint users (COCOM & Service Combatant) and have them define representative mission tasks.

With respect to the criteria/process to determine the appropriate representation (live, virtual, or constructive) of players in each engineering (DT or OT) event, the supporting players that constitute the system-of-systems for the Joint mission are determined on a case-by-case basis. The goal is for the system being inserted into the JME to be the most mature representation available. However, it is always a live system for IOT&E.

CH 8–3.28.3 Joint Mission Environment Lead Developmental T&E Organization

Scheduling all of the assets in the JME, especially live assets participating in exercises, proves a complex undertaking. A management and scheduling capability exists, and it is assumed the PM establishes a Lead DT&E Organization (or equivalent) for this purpose. The Lead DT&E Organization coordinates all LVC assets and the script of events, which is the plan for the specific JME missions incorporating acquisition systems under test in accordance with their schedules. Note that acquisition systems tend to have fixed decision points where unplanned delays could severely impact production. Finally, with a complex facsimile of a mission environment in place and acquisition systems scheduled to perform missions within it, additional programs may ask to "join in" the scheduled events for testing, training exercises, or other special events. This is encouraged, but the testing needs of the sponsoring program take precedence over the needs of other participants, and their participation should not interfere with the core purpose of the JME events.

CH 8–3.29 Testing of Corrosion Prevention & Control

Corrosion is defined as the deterioration of a material or its properties due to a reaction of that material with its chemical environment, based on DoDI 5000.67 (Para 3(b) – page 1). Corrosion of military equipment and facilities costs the DoD over $20 billion annually, and approximately 25 percent of all weapon systems maintenance is corrosion-related. Corrosion degrades system availability and safety. Based on safety and cost factors, it is beneficial to demonstrate the performance of corrosion prevention and control (CPC) on DoD systems. Therefore, DoDI 5000.67 (Para 4(b) – page 2) states that CPC programs and preservation techniques shall be implemented throughout the life cycle of all military equipment and infrastructure. Not only does CPC testing provide verification of system availability in meeting stated requirements, it can also validate and suggest improvements of repairs for corrosion events. If excessive corrosion is experienced, performance feedback can lead to corrective actions or better corrosion risk-mitigation activities.

In accordance with DoDI 5000.02 (Encl. 4, para 5(a)(6) – page 67), programs must identify the resource requirements for CPC developmental testing. Programs need to identify and provide the assets (e.g., test articles, test facilities, Manpower, Personnel and Training, funding) necessary to verify CPC performance. Conducting DT and OT concurrently helps with the cost and schedule of accomplishing CPC testing. System CPC testing is mostly covered during suitability testing for availability, maintainability, safety and environmental effects. As system or subsystem material modifications occur or the operating environment changes, programs should consider updating CPC testing.

In accordance with DoDI 5000.02 (Encl. 3, Para 15 – page 63), verification and acceptance tests are required for the corrosion prevention and control design. Since corrosion is a time-dependent problem, creativity is required in developing test methods. Assessing past test methods and results to identify best

practices and testing improvements for CPC is encouraged. The inclusion of corrosion subject matter expertise during T&E planning will ensure system corrosion test requirements are incorporated into system test plans. Conducting corrosion testing as early as practicable (starting with subassemblies and building up to full-scale articles) and potentially accelerating corrosion effects is critical, as the full effect of corrosion may not be seen until full-scale article testing or beyond.

At a minimum, CPC test requirements should be reflected in the Request for Proposal, Systems Engineering Plan (SEP), Life Cycle Sustainment Plan (LCSP), and Test and Evaluation Master Plan (TEMP), based on DoDI 5000.67 (Encl. 2, para 2(d)(1 & 2) – page 5).

For more information on corrosion prevention control, visit the DoD Corrosion and Prevention Control office at CorrDefense.org.

CH 8–4. Process Integration

This section describes how T&E supports the acquisition life cycle by phases, in accordance with DoDI 5000.02 (Encl. 4, para 2(b) – page 65). Involvement of T&E experts early in program planning better integrates T&E activities with the overall program planning and identifies the resources needed for the T&E program.

CH 8–4.1 Materiel Solution Analysis Phase

The purpose of this phase is to:

- Conduct the analysis and other activities needed to choose the concept for the product acquired.
- Translate validated capability gaps into system-specific requirements.
- Conduct planning to support a decision on the acquisition strategy for the product.

Key activities in this phase include:

- Designation of a Chief Developmental Tester and Lead DT&E Organization. in accordance with DoDI 5000.02 (Encl. 4, para 3(c) – page 65).
- Chartering a T&E WIPT and RAM IPT.
- Analysis of Alternative solutions.
- Key trades between cost and performance.
- Affordability analysis.
- Risk analysis.
- Planning for risk mitigation.
- Developing T&E strategy and plans.
- Review of threats and Intelligence Mission Data (IMD) identified or implied in the Integrated Threat Environment Assessment (ITEA) (NOTE: Soon to be replaced by the Validated Online Life-cycle Threat (VOLT)).

This phase ends when a Component has completed the necessary analysis and the activities necessary to support a decision to proceed to the next decision point and desired phase in the acquisition process. System testing does not occur before Milestone A.

CH 8–4.1.1 T&E Planning for Milestone A

Prior to completion of the Materiel Solution Analysis (MSA) Phase, the CAE selects a PM and establishes a program office to complete the necessary actions associated with planning the acquisition program. Additionally, a Chief Developmental Tester is identified as early as possible since the TMRR phase includes testing to support Milestone B, in accordance with DoDI 5000.02 (Encl. 4, para 3(c) – page 65).

The PM charters a T&E WIPT to assist in the T&E activities supporting a Milestone A decision (see CH 8–2.4.3 T&E Working-Level Integrated Product Team), in accordance with DoDI 5000.02 (Encl. 4, para 3(e) – page 66). The Chief Developmental Tester serves as chair of the T&E WIPT.

The Chief Developmental Tester is responsible for development of the Milestone A TEMP and participates in development of the Milestone A Acquisition Strategy. At Milestone A, an approved Acquisition Strategy and TEMP inform development of the final RFPs for the next phase of the program.

Milestone A TEMP. Projects that undergo a Milestone A decision have a T&E strategy documented in the TEMP, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(11) – page 68). Programs develop the initial TEMP during the Material Solution Analysis Phase in support of entry into Milestone A. The TEMP includes a description of the most promising system concepts, broad objectives, and an overall T&E strategy (including, DT&E, OT&E, and, if applicable, LFT&E). The Milestone A TEMP describes an evaluation methodology that provides essential information on programmatic and technical risks to inform the decision-maker. The evaluation methodology (and a framework, if needed) identify key data that contribute to assessing TMRR test assets (e.g., competitive prototypes, technology, etc.).

Programs derive the Milestone A TEMP and Evaluation Methodology from the Acquisition Strategy (AS), ICD, and draft CDD, including Enterprise architecture views, System Engineering Plan (SEP), Program Protection Plan (PPP), Critical Technical Parameters (CTP), and Analysis of Alternatives (AoA), and develop it in a collaborative environment utilizing the T&E WIPT. The WIPT assists in developing a T&E strategy describing how the capabilities in the ICD and draft CDD are tested and evaluated during system development. The TEMP leverages the ICD, draft CDD, and CONOPS/OMS/MP in order to have a firm understanding of the user requirements. The TEMP also takes into account the Systems Threat Assessment Report (STAR) and other acquisition products (e.g., SEP, PPP, etc.).

The Milestone A TEMP strategy evaluates system concepts against mission requirements. The T&E strategy in the TEMP includes the identification and management of associated risk, the use of modeling and simulation, and the identification of key resources.

The Milestone A TEMP includes sufficient information to describe in detail the T&E approach, focusing on the TMRR Phase, but also as far into the acquisition life cycle as feasible, based on information needs. The TEMP should consider the following information:

- Description of the developmental evaluation methodology that provides essential information on programmatic, technical risks, and major programmatic decisions, in accordance with DoDI 5000.02 (Encl. 4, para 5(a)(11) – page 68).
- Documentation of the T&E for phase completion that includes major test events required for milestone exit and entrance criteria.
- Description of each test phase or event.
- Identification of independent variables of significance affecting development, design, or operations.
- Assessment of the AoA assumptions and findings.
- Plan for evaluating prototypes, technology, etc.
- Documentation of the strategy and resources for cybersecurity T&E.
- Identification of the resources required to execute the planned T&E activities.
- Identification of the appropriate lessons learned concerning interoperability, test infrastructure, tools, and VV&A strategy.
- Documentation of the T&E program and master schedule for major T&E events.
- For MDAPs and MAIS, identification of the Chief Developmental Tester.
- For MDAPs, identification of the Lead DT&E Organization.
- Review of threats and Intelligence Mission Data (IMD) identified or implied in the STAR (soon to be replaced by the Validated Online Lifecycle Threat (VOLT)).

Refer to the TEMP Guidebook for more information.

T&E Role in Milestone A RFP. The evaluation strategy and an approved Acquisition Strategy inform development of the RFPs for any planned TMRR Phase contracts. A Chief Developmental Tester ensures the RFP adequately describes T&E management, evaluation requirements, T&E data management (including data rights), modeling and simulations, cybersecurity, T&E resources, and software management (during T&E execution). The RFP also includes reliability, availability, and maintainability (RAM) program requirements, including contractual design-for-reliability requirements. The Contract Data Requirements List (CDRL) identifies required contractor-generated test data, planned contractor T&E objectives and schedules, modeling and simulation to be used by contractor, verification and validation procedures, and planned contractor test facility acquisition.

Refer to Incorporating T&E into DoD Acquisition Contracts for more information.

CH 8–4.1.2 T&E Role in Milestone A Decision

The Milestone A decision approves program entry into the TMRR Phase. Prior to Milestone A approval, the Chief Developmental Tester ensures approval of the initial TEMP developed during the Materiel Solution Analysis (MSA) Phase, in accordance with DoDI 5000.02 (Encl. 4, para 3(a) – page 65). The RFP informs the Milestone A TEMP.

The responsible DoD Component may decide to perform technology maturation and risk reduction work in-house and/or award contracts associated with the conduct of this phase.

CH 8–4.1.2.1 Milestone A DT&E Program Assessment

For MDAPs, MAIS programs, and USD(AT&L)-designated special interest programs, the DASD(DT&E) will provide the MDA with a DT&E program assessment at the Milestone A Decision Point, in accordance with DoDI 5000.02 (Encl. 4, para 6(b) – page 68). The DT&E program assessment will be based on any DT&E activities completed to date as well as address the adequacy of the DT&E planning, DT&E strategy, DT&E schedule, developmental evaluation methodology, DT&E resources, and the risks to successfully meeting the goals of the DT&E activities in the Milestone A TEMP, in accordance with DoDI 5134.17 (Para 1(j) – page 4).

CH 8–4.1.3 Operational T&E Implications of CONOPS/OMS/MP

The Milestone A TEMP includes a discussion of the OT&E implications of the Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP). The OT&E implications discuss the missions and capabilities that the new system is intended to provide to using units, and how those new capabilities are assessed in OT&E. Any aspects of the CONOPS/OMS/MP that may require significant test assets, such as specialized units, target sets, ranges, threat emulators—threat models and simulations, threat actuals, intelligence mission data, or long production lead times—should be highlighted, in accordance with DoDI 5000.02 (Encl. 5, para 5(d) – page 71). The number of system units employed by the user in the context of an operational scenario (e.g., number of systems in a company), are identified to help scope the test program's resources. If the new system capability is intended to be applicable to a Joint force, the Joint aspects of the test program are considered here. If intended capabilities are to be fielded incrementally, the TEMP specifies which capabilities are tested in which test events. If applicable, the baseline against which the new system is judged is specified in the Milestone A TEMP, and resources allocated for the baseline testing as well as the new system testing.

Refer to the JCIDS Manual, Appendix B, Enclosure C, for more information on CONOPS.

CH 8–4.2 Technology Maturation & Risk Reduction Phase

In accordance with DoDI 5000.02 (Para 5(d)(4) – page 16), the TMRR phase mandates T&E support to help reduce technology, engineering, integration, and life-cycle cost risk of a program leading to three related decision points: CDD Validation Decision, Development RFP Release Decision, and the Milestone B Decision. The CDD Validation Decision informs decision-makers whether sufficient trades have been completed to support a decision to commit to the set of requirements for use in preliminary design

activities, development, and production (subject to reconsideration and refinement as knowledge increases). The Development RFP Release Decision informs decision-makers whether planning for development is complete and a decision can be made to release an RFP for development (and possibly initial production) to industry. The Milestone B Decision is the decision that commits the resources (authorizes proceeding to award of the contract(s)) needed to conduct development leading to production and fielding of the product.

CH 8–4.2.1 T&E Execution during Technology Maturation & Risk Reduction

The Acquisition Strategy and the Milestone A TEMP guide this acquisition phase. The Chief Developmental Tester, in collaboration with the T&E WIPT, monitors the execution of the T&E events and reviews T&E reports, in accordance with DoDI 5000.02 (Encl. 4, para 3(a) & 3(b) – page 65). Multiple technology development demonstrations/evaluations, defined in the Acquisition Strategy (AS) and the TEMP, may prove necessary before the user and developer can substantiate a preferred solution is feasible, affordable, and supportable; satisfies validated capability requirements; and has acceptable technical risk. Programs identify critical program information during this phase as well as implement program protection measures to prevent disclosure of critical information.

Contractor DT&E. During early DT&E, the contractor approach includes tests and evaluations for optimizing designs and functionalities. The contractor may also use modeling and simulation, laboratory, test bench, and system mock-ups or prototypes to gain knowledge of integrated system performance. Government T&E organizations may observe the critical contractor testing, conduct additional T&E, and, when practical, facilitate early user involvement. The government may be able to utilize contractor data to enhance or replace planned government testing, and to enable T&E efficiencies to be realized if testing is observed by a government T&E organization. The TMRR contract with industry should support open communication between government and contractor test organizations.

Government DT&E. During early DT&E, the Chief Developmental Tester uses government testing to evaluate competitive prototypes, competing technologies, technology maturity of critical technology elements, etc. The Lead DT&E Organization conducts developmental testing and evaluation activities for the program, as directed by the Chief Developmental Tester. The Lead DT&E Organization also ensures the AoA assumptions and findings are validated.

Early Operational Assessments. Early Operational Assessments (EOAs) provide a means to evaluate a program's progress early in the process towards developing an operationally effective, suitable, and survivable system, in accordance with DoDI 5000.02 (Encl. 5, para 6(a)(1) – page 72). EOAs are typically an analysis, based on a review of current program plans and documentation, as well as data from early developmental testing, technology assessments, modeling and simulation, and program reviews. EOAs enable the OTA to provide early input on key issues that, if not corrected, could have a detrimental effect to the determination of operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality. EOAs provide a means to examine the links and consistency between the concept of operations, requirements, and technology limitations to provide recommendations to the program and the requirements authority.

EOA reports are provided to support one or more of the design phase life-cycle events (namely, the CDD Validation Decision, the Development RFP Release Decision, or Milestone B). For programs entering development at Milestone B, the lead OTA (as appropriate) prepares and reports EOA results after program initiation and prior to the Critical Design Review (CDR).

CH 8–4.2.2 T&E Support during Technology Maturation & Risk Reduction

The TMRR phase includes activities intended to reduce the specific risks associated with the functions, technologies, environments, and developed products. This includes additional design trades and requirements necessary to ensure an affordable product and an executable development, production, and sustainment program.

Logistics Risk Assessment. During the TMRR phase, programs conduct a logistics risk assessment as part of life-cycle considerations. The PM finalizes sustainment requirements for approval at the CDD Validation Decision, and decomposes sustainment requirements into more detailed requirements to support the Preliminary Design Review (PDR) and for use during the logistics risk assessment. The T&E WIPT leverages the logistics risk assessment during development of the Milestone B TEMP.

Refer to the DAG, CH 4, Life Cycle Logistics for more information.

Technology Readiness Assessment (TRA). The TRA is a systemic, metric-based process that establishes the maturity of critical technologies. The TRA may be conducted concurrently with other technical reviews. The Chief Developmental Tester assists the chief engineer/lead systems engineer when assessing the technological maturity and integration risk of critical technologies.

Refer to the DAG, CH 3.4.1.3., Technical Assessment Process, for more information.

Preliminary Design Review (PDR). Conducted after preliminary design efforts, but before the start of detail design, the PDR provides the first opportunity for the DoD to closely observe the contractor's hardware and software design. The contractor describes all design changes made with respect to trade studies, design considerations, and design decisions that provide a rationale for the system's preliminary design. The contractor also provides a hardware or hands-on demonstration of some of the preliminary designs to better illustrate important aspects. The Chief Developmental Tester provides developmental test data collected to date to support the PDR. Test organizations attend technical reviews to provide current assessments, keep abreast of program progress, and provide insight into design direction. Unless waived by the MDA, the Preliminary Design Review occurs prior to Milestone B.

Refer to the DAG, CH 3.3.3.4., Preliminary Design Review, for more information.

Capability Development Document (CDD) Validation. In accordance with DoDI 5000.02 (Para 5(d)(4)(b) – page 16), the Technology Maturation and Risk Reduction (TMRR) Phase requires continuous and close collaboration between the program office and the requirements validation authority. During this phase, the Requirements Authority for the program validates the final CDD in order to provide a basis for preliminary design activities and the Preliminary Design Review, which normally occurs prior to Milestone B unless waived by the MDA. Prior to validation, the program coordinates the Capability Development Document (or other draft requirements document) with the MDA to ensure requirements remain technically achievable and affordable. The T&E WIPT reviews the draft CDD and coordinates the input with the PM. This effort provides the T&E WIPT a key opportunity to review requirements, to determine if they are clear, testable, measurable, and technically achievable.

Refer to the DAG, CH 4.3.2.3.1., Capability Development Document, for more information.

CH 8–4.2.3 Development RFP Release Decision

Prior to the Development Request for Proposal (RFP) Release Decision, and prior to release of a request for proposal (RFP) for the Engineering and Manufacturing Development (EMD) phase, the PM submits the Acquisition Strategy (AS) and obtains MDA approval. The approved Acquisition Strategy informs development of the RFPs for Engineering and Manufacturing Development contracts.

The Chief Developmental Tester, in collaboration with the T&E WIPT, provides a draft Milestone B TEMP ("draft" means a DoD Component-approved draft) at the Development RFP Release Decision, in accordance with DoDI 5000.02 (Encl. 1, Table 2 – page 34).

The Development RFP Release Decision ensures, prior to the release of the solicitation for Engineering and Manufacturing Development, an executable and affordable program has been planned using a sound business approach. The goal is to avoid any major program delays at Milestone B, when source selection is already complete and award is imminent. Prior to release of the final RFP(s):

- There needs to be confidence that the program requirements to be bid against are firm and clearly stated.
- The risk of committing to development and presumably production has been or is adequately reduced prior to contract award and/or option exercise.
- The program structure, content, schedule, and funding are executable and the business approach and incentives are structured to both provide maximum value to the government and treat industry fairly and reasonably.

The T&E WIPT assists in RFP development to ensure it addresses key T&E requirements identified in the TEMP.

The Development RFP Release Decision authorizes the cognizant DoD Component to release an RFP to industry.

The RFP for EMD needs to address the contractor T&E activities across the programs that are critical for program success.

RFPs should address T&E-related needs, such as:

- Evaluation strategy
- Test articles
- T&E data rights
- Government access to:
  - Contractor test and evaluation data on system performance, interoperability, reliability, and cybersecurity, and, (if mission critical), nuclear effects survivability
  - Failure Reporting, Analysis, and Corrective Action System
  - Other test-related data/results or repositories
- Built-in test and embedded instrumentation (including software log files)
- Government use of contractor-conducted T&E
- Government review and approval of contractor T&E plans
- Government witness of contractor test events
- Government review of contractor evaluations
- Verification, validation, and accreditation of modeling and simulation to be used, including threats and threat environments
- Investment in contractor-owned test facilities
- Adjudication process for reliability, availability, and maintainability data
- Contractor participation in the T&E WIPT
- An Industry Test Lead, included in the key personnel clause, to participate and interact with the Chief Developmental Tester and Lead DT&E Organization
- Meta-data, formats, and specific data requirements are included in the Contract Data Requirements List (CDRL).

Refer to "Incorporating T&E into DoD Acquisition Contracts" for more information.

CH 8–4.2.4 T&E Master Plan at Milestone B

The TEMP at Milestone B focuses on the overall structure, major elements, and objectives of the T&E program. If applicable, the TEMP contains a mature strategy that commits to full-up, system-level, live fire testing, or a waiver request is submitted and approved for the LFT&E plan. The T&E WIPT plans and executes system modeling, simulation, and T&E activities into an integrated and efficient continuum. Per DoDI 5000.02 (Encl. 4, para 5(a)(11) – page 68), the TEMP at Milestone B will include a developmental evaluation framework.

Typical T&E planning activities supporting a Milestone B TEMP include:

- Determining types and quantities of data for collection and evaluation.
- Estimating the anticipated test risks/results through simulation and modeling.
- Establishing safe test procedures.
- Ensuring adequate environmental protections.
- Projecting resource and schedule requirements, including simulated threat environments and targets.
- Other planning activities, as identified in the TEMP Format.

The program must update the TEMP prior to each subsequent milestone decision.

A program may create the Milestone B TEMP based on an updated Milestone A TEMP. In accordance with DoDI 5000.02 (Encl. 4, para 5(c) – page 68), a program submits a DoD Component-approved draft not later than 45 days prior to the milestone decision. For Information Systems Acquisition, the Milestone B TEMP serves as a planning document for the IOT&E of limited fieldings.

CH 8–4.2.5 T&E Planning for Milestone B

The TEMP at Milestone B includes T&E information informing a variety of decisions, including:

- Planning Decisions: What T&E is performed and how to phase it to support system development and design?
- Management Decisions: Is the system ready to transition to the next development phase with associated exit criteria achieved and entrance criteria identified?
- Design Decisions: Is technical performance as planned, including assessment of design margin? If not, how can we improve performance?
- Contractual Decisions: How is performance best verified and does it work as specified?
- Logistical Decisions: What T&E must be performed to ensure the system, subsystems, and components are designed for reliability, maintainability, and supportability, and remain reliable, maintainable, and supportable?
- Acquisition Decisions: What T&E data are needed to support the decision?
- Intelligence Mission Data: What data are available?

The PM identifies DT&E phases or events in the TEMP as contractor or government DT&E. Contractor and government DT&E should provide a continuum that provides confidence in the system, subsystem, and component design solutions. Major DT&E phases and events are planned with a test readiness review (TRR) that includes entrance and exit criteria. Integrated testing can also provide confidence in the system, subsystem, and component design solutions.

In accordance with DoDI 5000.02 (Encl. 4, para 5(b) – page 68), programs will utilize government T&E capabilities, unless the program can identify a cost-effective exception. Additionally, programs must conduct a Cost Benefit Analysis (CBA) for exceptions to this policy, and document the assumptions and results of the CBA in the TEMP before acquiring non-government program-unique test facilities or resources.

The TEMP includes one or more reliability growth curves for reliability risk capabilities, components, and subcomponents, as appropriate. Growth program plans also include identification of contractor design for reliability activities.

CH 8–4.2.6 T&E Reporting in Milestone B Decision

The risk associated with a Milestone B decision is based on evaluations of any available test data and test reports. In accordance with DoDI 5000.02 (Encl. 4, para 6(c)(1) – page 69), DASD(DT&E) will have full and prompt access to all ongoing developmental testing, developmental test records, and test reports for all MDAP/MAIS programs. Prompt access allows DASD(DT&E) to conduct assessments in the TMRR phase for:

- Technology maturity
- Performance of Critical Technology Element (CTEs) to meet CTPs or other performance parameter thresholds
- Adequacy of executing the test plan submitted for the TMRR phase
- Risk reduction
- Request for Proposal (RFP)
- Adequacy of test plan for EMD phase.

CH 8–4.2.7 T&E Role in Milestone B Decision

Milestone B serves as the point at which a program is reviewed for entrance into the Engineering & Manufacturing Development (EMD) phase. In accordance with DoDI 5000.02 (Para 5(c)(2)(b)(4)(a) – page 7), the role of T&E at Milestone B is to inform the Milestone Decision Authority (MDA) as to whether the:

- Risks (technology, engineering, integration, safety, etc.) are understood and have been adequately mitigated.
- System has met or exceeds all T&E-related TMRR phase exit criteria.

CH 8–4.2.7.1 Milestone B DT&E Program Assessment

DASD(DT&E) conducts a DT&E Program Assessment for all MDAPs, MAIS, and programs designated as AT&L Special Interest, in accordance with DoDI 5000.02 (Encl. 4, para 6(b) – page 68). The DT&E Program Assessment bases its findings and recommendations on the results of all program T&E to date, including contractor and government DT&E, integrated tests, certifications, and prior operational assessments(s). The DT&E Program Assessment at Milestone B focuses on evaluating critical technology performance and maturity, risk reduction, and whether a program's planning, schedule, and resources are adequate to support future DT&E.

CH 8–4.2.7.2 Operational Test Agency Report of Operational Test and Evaluation Results

The program may include Early Operational Assessments (EOAs), as appropriate, in accordance with DoDI 5000.02 (Para 5(c)(2)(b)(4)(a) – page 7). The appropriate operational test activity reports the results to the Service Chief, and the MDA can also use the results in support of decisions.

CH 8–4.3 Engineering & Manufacturing Development Phase

The purpose of the EMD phase is to develop, build, and test a product to verify all operational and derived requirements have been met, and to support production or deployment decisions, in accordance with DoDI 5000.02 (Para 5(c)(2)(b)(3) – page 6).

CH 8–4.3.1 T&E Execution during Engineering & Manufacturing Development

In accordance with DoDI 5000.02 (Encl. 4, para 4(b) – page 66), DT&E activities include assessing the ability of the system, subsystem, and components to meet their stated, derived, and allocated requirements in a mission-oriented context. This includes assessment of design margin, technical

parameters, and the approved KPPs in support of development, system production, and fielding. The effort requires completion of DT&E activities consistent with the TEMP, and may include operational assessments. Successful completion of adequate DT&E with production or fielding representative prototype test articles normally provides the basis for entering LRIP or Limited Fielding.

Contractor DT&E. Programs continue to utilize contractor-conducted DT&E and contractor-owned test facilities during EMD, as specified in the contract and Contract Data Requirements List (CDRL). The PM uses the TEMP as a source document when developing the request for proposal (RFP).

Government DT&E. In accordance with DoDI 5000.02 (Encl. 4, para 4(b) – page 66), the program executes government DT&E in order to validate the system to date in such areas as:

- Achievement of critical technical parameters and the ability to achieve key performance parameters.
- Assessment of the system's ability to achieve the thresholds.
- Assessment of the system's capabilities, limitations and deficiencies.
- Assessment of the system's safety.
- Assessment of the system's cybersecurity.
- Assessment of the system's ability to achieve interoperability certification.

Government DT&E not only verifies that the system meets the specification requirements, but also identifies the system's capabilities and limitations. If users are not available to support contractor human factors engineering tests, it is even more important that they participate in government DT&E. The TEMP describes a mission-oriented approach to DT&E that utilizes actual users in a mission context. The users are made available during DT&E to identify, early on, any deficiencies. The earlier deficiencies are found, the less cost and negative impact they have on the program. The mission-oriented approach also supports integrated testing to share test data among many stakeholders.

Development delays pose a schedule risk for DT&E. The Chief Developmental Tester should remain alert to the compression of test schedules and characterize the risk based on the information contained in the DEF. Test planning and execution may also generate schedule risks. The Chief Developmental Tester develops a detailed test schedule starting with the Test Readiness Review (TRR) immediately prior to test execution and works backward to capture all the tasks and resources for multiple internal and external sources needed to have a successful TRR decision, in accordance with DoDI 5000.02 (Encl. 4, para 6(a) – page 68). One or more senior-level intermediate TRRs are scheduled prior to the final TRR to assess progress and focus efforts on resolving issues. A schedule is developed from the last TRR forward to capture all the test execution and reporting tasks necessary to support the EMD and Milestone C decisions.

MDAP programs utilize their designated Lead DT&E Organization to support the Chief Developmental Tester in the planning, execution, and assessment of DT&E.

Operational Assessment (OA). An operational assessment is a test event conducted before initial production units are available and which incorporates substantial operational realism. An OA is conducted by the lead operational test agency (OTA) in accordance with a test plan approved by the Director, Operational Test and Evaluation (DOT&E) for programs subject to Office of the Secretary of Defense (OSD) operational test and evaluation (OT&E) oversight. As a general criterion for proceeding through Milestone C, the lead OTA will conduct and report results of at least one OA. An OA is usually required in support of the first limited fielding for acquisition models employing limited fieldings. An operational test, usually an OA, is required prior to deployment of Accelerated Acquisition Programs that are subject to OSD OT&E or Live Fire Test and Evaluation (LFT&E) oversight. An OA may be combined with training events. An OA is not required for programs that enter the acquisition system at Milestone C.

Low-Rate Initial Production (LRIP). Successful completion of adequate developmental testing with production or fielding representative prototype test articles normally serves as the basis for entering LRIP or Limited Fielding. DoDI 5000.02 (Encl. 4, para 6(a) – page 68) includes more detailed discussions of T&E requirements.

CH 8–4.3.2 Operational Test Agency Report of Results of Operational Assessment

Operational Assessments (OAs) provide a means to evaluate early in a program's life cycle, progress towards developing an operationally effective, suitable, and survivable system. OAs are based on a review of current program progress and documentation as well as data from test events that incorporate substantial operational realism to provide an assessment of mission capability under operationally realistic conditions. OAs can include dedicated early operational testing, and/or Limited User Testing as well as developmental test results, provided they are conducted with operational realism. OAs are developed to support Milestone C and Low-Rate Initial Production (LRIP) decisions, in accordance with DoDI 5000.02 (Encl. 5, para 4(b) – page 70). OAs serve to identify system deficiencies early that, if not corrected, could have a detrimental effect on the future determination of operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality, and/or survivability. In addition to identifying operationally critical system capabilities, risks to program success, and system limitations and deficiencies, OAs provide recommendations to the program on system improvements, suggested updates to requirements and concept of operations, and needed changes to the test program to ensure adequate testing prior to full-rate production decision or full-deployment decision.

CH 8–4.3.3 Live Fire Test & Evaluation

Live Fire Test and Evaluation (LFT&E) encompasses testing and evaluation over the course of a program, beginning with component-level testing during the initial design stage. T&E continues as the system matures from assemblies to subsystems, and finally to a full-up, system-level configuration. At the full-up, system-level, the weapon system is fully equipped for combat with all subsystems operational and powered. Early identification of deficiencies through LFT&E allows time to impact design trades and make design changes before finalizing production configurations, thereby reducing costs. Survivability and lethality testing conducted under the auspices of the LFT&E program generate information that directly supports the DOT&E mission of evaluating the operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality of major defense acquisition programs, in accordance with DoDI 5000.02 (Encl. 5, para 9 – page 74).

The test organization responsible for LFT&E events prepares a detailed test plan. The DoD Component and the Director, Operational Test and Evaluation (DOT&E) approve TEMPs, operational test plans, and live fire test plans. For programs under DOT&E oversight, the DOT&E provides the MDA with LFT&E assessments, in accordance with DoDI 5000.02 (Encl. 1, Table 2 – page 36).

Refer to DAG CH 8.3.2.5., Live Fire Test & Evaluation for more information.

CH 8–4.3.4 T&E Support during Engineering & Manufacturing Development

Entrance into the Engineering and Manufacturing Development (EMD) phase depends on technology maturity demonstrated during the TMRR phase, approved requirements, and full funding. The EMD phase effectively integrates T&E with the acquisition, engineering, and manufacturing processes. Developmental (government and contractor) and operational test agencies integrate seamlessly during this phase. The Chief Developmental Tester ensures the T&E program depth, breadth, and phasing remain adequate to uncover risks throughout the performance envelope to manage risks at the Milestone C LRIP decision, in accordance with DoDI 5000.02 (Encl. 4, para 3(a) – page 65).

Critical Design Review (CDR). The Critical Design Review assesses design maturity, design build-to documentation, and remaining risks, as well as establishing the initial product baseline. The CDR serves as the decision point signifying the system design has matured so that hardware fabrication can begin, with acceptable risk. The Chief Developmental Tester and the Lead DT&E Organization should attend the

CDR and provide an up-to-date assessment of the system. During the development of the TEMP, the Chief Developmental Tester discusses the assessments needed for the CDR with the System Engineer.

Refer to CH 3.3.3.5., Critical Design Review, for more information on the CDR.

Long Lead Items. The milestone decision authority (MDA) may authorize the production of long lead items for LRIP or full production during Engineering and Manufacturing Development (EMD), subject to the availability of appropriations. Procurement of long lead items in advance of a Milestone C production decision provides items for T&E purposes and a more efficient transition to production. The amount of long lead items appropriate for a given program depends on the type of product acquired. The product's content dictates the need for early purchase of selected components or subsystems to affect a smooth production process. The MDA may authorize long lead items at any point during EMD, including at Milestone B. An authorized Acquisition Decision Memorandum (ADM) documents long lead items, along with any limits in content (i.e., listed items) and/or dollar value.

DOT&E approves the quantity of items for programs on oversight and the MDA authorizes the minimum LRIP quantities needed to provide production representative test articles for OT&E and to maintain continuity in production pending OT&E completion, in accordance with DoDI 5000.02 (Encl. 5, para 10(d) – page 74). For systems not on the DOT&E Oversight List for OT purposes, the OTA, following consultation with the PM, determines the number of test articles required for IOT&E. In accordance with 10 USC 2400. The program includes the LRIP quantity for an MDAP (with rationale for quantities exceeding 10 percent of the total production quantity documented in the acquisition strategy) in the first Selected Acquisition Report (SAR) submitted to Congress after its determination.

CH 8–4.3.5 T&E Planning for Milestone C

Milestone C is the point at which a program is reviewed for entrance into the Production and Deployment (P&D) phase. Approval depends on specific criteria defined at Milestone B and included in the Milestone B ADM. In accordance with DoDI 5000.02 (Para 5(d)(10)(a) – page 21) for Milestone C approval, the following general criteria apply:

- An approved Acquisition Strategy (AS).
- Demonstration that the production design is stable and meets stated and derived requirements based on acceptable performance in developmental test.
- An operational assessment.
- Mature software capability consistent with the software development schedule.
- No significant manufacturing risks.
- A validated final requirements document (normally a Capability Production Document (CPD)).
- Demonstrated cybersecurity.
- Demonstrated interoperability.
- Demonstrated operational supportability.
- Costs within affordability caps.
- Full funding in the Future Years Defense Program (FYDP).
- Properly phased production ramp up and/or fielding support.

TEMP at Milestone C. The Milestone C TEMP is an update of the Milestone B TEMP, including the developmental evaluation framework, in accordance with DoDI 5000.02 (Encl. 1, Table 2 – page 38). The Milestone C TEMP contains an updated T&E strategy for IOT&E. The program demonstrates the stability of production design and meets stated and derived requirements based on acceptable performance in developmental test, in accordance with DoDI 5000.02 (Encl. 5, para 5(c)(2) – page 71). Updated reliability growth curves at Milestone C reflect test results to date and any updates to the reliability growth plan.

Incremental Software Capability programs (and other acquisition models that do not have a Milestone C) are, in some cases, asked to provide an operational test plan for IOT&E.

RFP at Milestone C. Given the maturity of the program at this stage in the acquisition cycle, programs may need to update the RFP accordingly. The updated RFP may include changes to T&E requirements. The RFP is consistent with the Milestone C TEMP, CPD, Acquisition Strategy (AS), etc.

CH 8–4.3.6 T&E Reporting in Milestone C Decision

Development of the MDA position on the risk of a Milestone C approval for initiating Production is based on:

- Evaluations of DT and OT (if applicable) results from the preceding EMD phase, including consideration of how thoroughly the system was stressed during EMD (mission-oriented context and operationally realistic environments).
- Assessment of the risk of a design change affecting production.
- Adequacy of the DT&E planning (e.g., requirements that can be evaluated, TEMP adequacy and currency, developmental evaluation framework, DT&E schedule, test resources availability, and modeling and simulation evaluated for mission capabilities) for the remaining P&D phase.

In accordance with DoDI 5000.02 (Para 5(d)(10)(a) – page 21), T&E support of Milestone C entrance criteria includes:

- Evaluations of DT results.
- OA results.
- Security Assessment Report provided by the SCA.
- Any applicable certifications required (e.g., airworthiness, safety, etc.).

Based on the DT&E and OA results of EMD, reporting substantiates:

- Performance in DT&E.
- Test results that demonstrate a readiness for production.
- Mature software capability.
- Interoperability.
- Operational supportability.
- Cybersecurity.

CH 8–4.3.7 T&E Role in Milestone C Decision

Milestone C serves as the point at which a program is reviewed for entrance into the Production and Deployment Phase. In accordance with DoDI 5000.02 (Para 5(d)(10)(a) – page 21), the role of T&E at Milestone C is to inform the MDA as to whether the:

- Design is stable.
- System meets validated capability requirements.
- System has met or exceeds all directed EMD phase exit criteria.
- DT&E results support an initial production decision.
- OT&E results support an initial production decision

DT&E activities may continue past the initial production or fielding decision until requirements have been tested and verified.

CH 8–4.3.7.1 Milestone C DT&E Program Assessment

DASD(DT&E) conducts a DT&E Program Assessment at Milestone C for all MDAPs, MAIS, and programs designated as AT&L Special Interest, in accordance with DoDI 5000.02 (Encl. 4, para 6(b) – page 68). The MDA considers the results of the DT&E Program Assessment when making a determination of materiel system readiness for production. The DT&E Program Assessment bases its findings and recommendations on the results of testing to date, including: full-up system level DT&E, integrated tests, certifications, and prior operational assessments(s). The DT&E Program Assessment at Milestone C evaluates system performance (against key performance measures (e.g., KPPs, KSAs, CTPs, etc.)), reliability and/or availability, interoperability, and cybersecurity. DASD(DT&E) provides an updated DT&E Program Assessment prior to proceeding to IOT&E.

CH 8–4.3.7.2 Operational Test Agency Report of OT&E Results

In accordance with DoDI 5000.02 (Encl. 5, para 6(a)(2) – page 72), the Operational Test Agency (OTA) provides an OTA Report of OT&E results, based on OT conducted to date, in support of the Milestone C Decision. The OTA Report focuses on:

- Progress toward operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality.
- Significant trends noted in development efforts.
- Programmatic voids.
- Risk areas.
- Adequacy of requirements.
- The ability of the program to support adequate operational testing.

CH 8–4.4 Production & Deployment Phase

The Production and Deployment (P&D) phase produces and delivers requirements-compliant products to receiving military organizations.

The P&D phase begins with an LRIP or production/procurement decision by the MDA. LRIP initiates the manufacturing capability and also provides the production-representative systems for IOT&E, in accordance with DoDI 5000.02 (Para 5(d)(11)(b)(2) – page 22). LRIP efforts end when the MDA either terminates the program or approves FRP after determining the program demonstrates sufficient control of the manufacturing process along with acceptable system characteristics.

The P&D phase focuses on achieving an operational capability satisfying mission needs. Except as specifically approved by the MDA, programs have resolved or identified a funded resolution plan before proceeding beyond LRIP. Earlier DT&E has had the system operating in mission-oriented environments with sufficient operational realism ensuring the identification and correction of deficiencies prior to IOT&E.

Production Representative Test Articles. Operational test and evaluation (OT&E) requires production representative test articles. The TEMP lists the number of production representative test articles available for OT&E, which serves as part or all of the authorized LRIP quantity.

CH 8–4.4.1 T&E Execution during Production & Deployment

Test organizations are involved in the preparation for, and conduct of, DT&E during the P&D phase preceding IOT&E. If the DT&E during the preceding phases was designed to introduce the system under development to mission-oriented scenarios in operationally realistic environments, system capabilities and limitations are evident by now. The last DT&E preceding IOT&E includes the demonstration and verification of any corrections of deficiencies evidenced during earlier DT work, in accordance with DoDI 5000.02 (Encl. 4, para 4(b)(16) – page 66). The focus on mission analysis and the system's contribution to the mission imply that evaluations are not based solely on the extent to which a system meets KPPs

and criteria accompanying critical issues. In addition to assessing how well system performance meets standards, test organizations also assess the system's contribution to accomplishing the overall mission.

DT&E. The Chief Developmental Tester plans for and ensures execution of DT events deemed necessary to address any remaining DT&E issues in order to assess entry into IOT&E and FRP.

IOT&E. The Service OTA conducts the IOT&E, executing the planned events based on the approved test plan, in accordance with DoDI 5000.02 (Encl. 5, para 11(a)(8) – page 76) and DoDI 5000.02 (Encl. 1, Table 2 – page 36).

LFT&E. The Service OTA or assigned test activity conducts the LFT&E, executing the planned events based on the approved LFT&E Plan, in accordance with DoDI 5000.02 (Encl. 5, para 11(b)(1) – page 76).

First Article Testing (FAT) and Acceptance Testing (AT). FAT and AT are two important test execution events during P&D. They are normally conducted by the contractor, using government-approved test plans and under the oversight of government personnel resident at the contractor facility (e.g., Defense Contract Management Agency (DCMA)) or project management office (PMO) personnel. As part of FAT, which tests the production processes, environmental stress screening (ESS), such as highly accelerated life testing (HALT), is conducted to identify and eliminate production flaws, such as bad soldering/welding, poor seal installation, etc. FAT may also test selected performance measures to ensure the production process does not degrade performance from earlier test findings. FAT is conducted expeditiously because the production line may continue to flow while FAT results are determined. AT is conducted on every delivered system and may be a limited functional test to ensure each system is properly working. It is important because it is the point where the government accepts ownership and responsibility of the system. It may also serve as the start point for the warranty coverage. The Chief Developmental Tester reviews and understands the contract details regarding FAT and AT.

FOT&E. FOT&E is conducted to complete unfinished IOT&E activity and evaluate major technical changes made to the system to correct identified deficiencies in the IOT&E. FOT&E evaluates whether or not the system continues to meet operational needs and retains operational effectiveness in a substantially new environment, as appropriate. It also provides a venue to address any OT&E and/or OTA recommendations provided in the IOT&E report.

CH 8–4.4.2 T&E Support during Production & Deployment

Except as specifically approved by the MDA, critical deficiencies identified in EMD testing are resolved prior to proceeding beyond LRIP or Limited Deployment. Any remaining DT&E included in the Milestone C TEMP is conducted prior to proceeding to IOT&E. The Chief Developmental Tester and Lead DT&E Organization are involved in the preparation for, and conduct of, any remaining DT&E that precedes IOT&E, in accordance with DoDI 5000.02 (Encl. 4, para 4(b)(16) – page 66). Over the system life cycle, operational needs, technology advances, evolving threats, plans for system upgrades/improvements (e.g. engineering change proposals (ECPs), etc.), or a combination of these items may require a TEMP to describe the associated test program.

CH 8–4.4.3 T&E Planning during Production & Deployment

T&E activities include:

- Reviewing and updating TEMPs, as required.
- Updating VV&A plans.
- Updating and coordinating DT&E test plans, if necessary.
- Updating and coordinating OTA test plans.
- Reviewing intelligence, threat, and CONOPS/OMS/MP documents for changes.
- Preparing DT&E Program Assessment and OT reports.
- Supporting OTRRs.

Updated TEMP. After the full rate production decision or the full deployment decision and thereafter, DOT&E and/or DASD(DT&E) may direct the DoD Component Acquisition Executive (CAE) to provide TEMP updates or addenda to articulate additional testing (e.g., FOT&E, Verification of Correction of Deficiencies periods, test program for future increments). The OTA may also request TEMP updates or addenda to articulate additional testing. DoDI 5000.02 (Encl. 1, Table 2 – page 38) provides additional information.

Test Articles for FOT&E (if required). DOT&E approves the quantity of test articles required for all OT&E test events for any system under OSD OT&E oversight, in accordance with DoDI 5000.02 (Encl. 5, para 9 – page 74). For programs not on DOT&E oversight, the OTA determines the quantity of test articles required for all OT&E events, in accordance with 10 USC 2400.

T&E planning is also concerned with determining the mix of T&E best suited for a system's production qualification, production acceptance, and sustainment. The DCMA or government-equivalent representatives and procedures may encompass the production evaluations at the contractor's manufacturing site, or may require the T&E effort to establish and mature the processes. Therefore, the appropriate level of evaluation could range from none, for normal DCMA practices, to minimal for first article qualification checks, to more extensive evaluations based upon production qualification test (PQT) results for new or unique manufacturing techniques, especially with new technologies.

Refer to the DAG, CH 10.3.2.1.2.2., Quality Assurance Surveillance Plan, for information on Government Contract Quality Assurance (GCQA).

CH 8–4.4.4 T&E Role during Production & Deployment

Operational Test Agency Report of OTA Results. The appropriate operational test agency conducts operational testing with LRIP units. After test completion, the Service OTA provides an independent report assessing the operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality of the system. For oversight programs, the Service OTA provides the report to DOT&E.

Beyond LRIP Report. The Director, DOT&E provides the MDA, Secretary of Defense, and Congress with a Beyond LRIP Report documenting the results of OT&E and providing the Director's determination of whether the program proves operationally effective, operationally suitable, and survivable, in accordance with DoDI 5000.02 (Encl. 5, para 1(c) – page 69). For programs on the DOT&E Oversight List, operational testing occurs in accordance with the DOT&E-approved TEMP.

Refer to DoDI 5000.02, Encl. 5 for more information.

Full Rate Production (FRP). The MDA conducts a review to assess the results of initial OT&E, initial manufacturing, and initial deployment, and then determines whether or not to approve the program's proceeding to Full-Rate Production and/or Full Deployment, in accordance with DoDI 5000.02 (Encl. 5, para 5(b) – page 70). Continuing to Full-Rate Production and Deployment requires demonstrated control of the manufacturing process, acceptable performance and reliability, and the establishment of adequate sustainment and support systems.

CH 8–4.5 Operations & Support Phase

The operations and support (O&S) phase focuses on executing the product support strategy, satisfying materiel readiness and operational performance requirements, and sustaining the system in the most cost-effective manner over its total life cycle (including disposal).

O&S has two major efforts: life cycle sustainment and disposal, in accordance with DoDI 5000.02 (Para 5(d)(14)(b) – page 23). Effective sustainment of systems results from the design and development of supportable, reliable, and maintainable systems. Sustainment strategies can evolve throughout the system's life cycle. The PM works with system users to document performance and sustainment

requirements in agreements specifying objective outcomes, measures, resource commitments, and stakeholder responsibilities. The Services, with system users, conduct continuing reviews of sustainment strategies to compare performance expectations against actual performance measures. The program disposes of the system in an appropriate manner when it reaches the end of its useful life.

CH 8–4.5.1 T&E Support during Operations & Support

During the support phase, the Chief Developmental Tester focuses on:

- Regression testing and evaluation of test articles that incorporate operationally significant improvements, modifications, and corrective actions prior to fielding improvements and modifications.
- Routine T&E of routine technical changes to all components and subcomponents.
- Demonstration of the maturity of the production process through production qualification testing (PQT) and production readiness review (PRR).
- Demonstration of the maturity of the software maintenance processes (if not completed in IOT&E or FOT&E).
- Surveillance testing.
- Shelf-life extension testing.

The PM may initiate system modifications, as necessary, to improve performance and reduce ownership costs. Test organizations remain aware of system modifications, review TEMP updates, and ensure PMs consider disposal during the design process, in accordance with DoDI 5000.02 (Encl. 5, para 5(b) – page 70). PMs document hazardous materials contained in the system in the programmatic environment, safety, and occupational health evaluation (PESHE) as well as estimate and plan for the system's demilitarization and safe disposal. The PM also considers the demilitarization of conventional ammunition during system design.

DOT&E determines when to remove a program from DOT&E oversight. Some of the typical reasons for removal include:

- A program is no longer in production.
- No additional follow-on operational testing.
- The program office is disbanded.
- Significant upgrades are no longer considered.

CH-8 Version and Revision History

Use the table below to provide the version number, the date that the particular version was approved and a brief description of the reason for and content changes contained in the revised version.

Version #	Revision Date	Reason
0	1 February 2017	DAG Chapter 8 Initial Upload.
1	6 April 2017	Section 8-3.7.4. Last sentence, removed hyperlink for "STAT" and corrected the URL for STAT COE.
2	5 July 2017	Updated DoDI 5000.02 page numbers to reflect Change 2.
3	25 September 2017	Updated several sections to include "Service intelligence organizations" when discussing threat requirements.

4	8 March 2018	Updated broken hyperlinks, made a few minor edits for content clarity.
5	20 June 2018	Updating Cybersecurity section.